

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD., and
SAMSUNG ELECTRONICS AMERICA, INC.,

Petitioner,

v.

Secure Wi-Fi LLC,

Patent Owner.

U.S. Patent No. 9,961,552

Inter Partes Review No.: IPR2024-01368

Inter Partes Review No.: IPR2024-01369

DECLARATION OF HARRY V. BIMS, PH.D.

TABLE OF CONTENTS

I.	Overview	1
II.	Experience and Qualifications	2
III.	Information and Materials Considered	4
IV.	Legal Framework	5
	A. Person of Ordinary Skill in the Art (“POSITA”)	5
	B. Claim Construction	6
	C. Obviousness	7
V.	Summary of Opinions	11
VI.	Person of Ordinary Skill in the Art	12
VII.	Technical Background	13
VIII.	The ’552 Patent	26
	A. The Subject Matter Described	27
	B. The Prosecution History	31
IX.	Overview of the Prior Art References	31
	A. Vardi	31
	B. Yun	33
	C. IEEE802.11	35
	D. Orava	37
	E. Kholaiif	38
	F. Motivation to Combine	39
	1. Vardi, IEEE802.11, Orava, and Yun	39
	G. Motivation to Combine	48
	1. Vardi, IEEE802.11, Orava, Yun, and Kholaiif	48
X.	Vardi, IEEE802.11, Orava and Yun Render Claims 1-9 Obvious	51
	A. Obviousness of Claims 1-9 (IPR2024-01368 Ground 1)	51
	1. Independent Claim 1	51

2.	Claim 2	71
3.	Claim 3	73
4.	Independent Claim 4	74
5.	Claim 5	93
6.	Claim 6	103
7.	Claim 7	104
8.	Claim 8	106
9.	Claim 9	109
XI.	Vardi, IEEE802.11, Orava and Yun Render Claims 10-28 Obvious.....	111
A.	Obviousness of Claims 10-28 (IPR2024-01369 Ground 1)	111
1.	Independent Claim 10	111
2.	Claim 11	155
3.	Claim 12	157
4.	Claim 13	158
5.	Claim 14	159
6.	Independent Claim 15	163
7.	Claim 16	168
8.	Claim 17	170
9.	Claim 18	171
10.	Claim 19	172
11.	Claim 20	174
12.	Independent Claim 21	178
13.	Claim 22	181
14.	Claim 23	183
15.	Independent Claim 24	184
16.	Claim 25	192
17.	Claim 26	193
18.	Claim 27	195
19.	Claim 28	196

XII.	IPR2024-01369 Ground 2: Vardi, IEEE802.11, Orava and Yun	
	Render Claims 24-28 Obvious	198
A.	Obviousness of Claims 24-28	198
1.	Independent Claim 24	198
2.	Claim 25	204
3.	Claim 26	204
4.	Claim 27	205
5.	Claim 28	205
XIII.	Conclusion.....	206

I, HARRY V. BIMS, PH.D., HEREBY DECLARE AS FOLLOWS:

I. OVERVIEW

1. I am over eighteen (18) years of age and otherwise competent to make this declaration.

2. I have been retained as an expert on behalf of Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (“Petitioner”) in connection with the above-captioned *inter partes* review of U.S. Patent No. 9,961,552 (“’552 patent”). Ex. 1001.

3. I am being compensated for my time spent on this matter at my standard rate of \$700 per hour. My compensation is not contingent upon the substance of my opinions, my testimony, or the outcome of the *inter partes* review proceeding.

4. I am not currently, and have not at any time in the past been, an employee of Petitioners or any affiliate or subsidiary thereof. I have no financial interest in Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.

5. I have been asked to provide my opinions regarding whether claims 1-28 of the ’552 patent are invalid as obvious to a person having ordinary skill in the art at the time of the alleged invention (“POSITA”).

6. This declaration summarizes the opinions I have formed to date. I reserve the right to modify my opinions, if necessary, based on further review and analysis of information that I receive subsequent to the filings of this declaration,

including in response to evidence or positions that parties to the *inter partes* review proceeding, or other experts, may take that I have not yet seen.

II. EXPERIENCE AND QUALIFICATIONS

7. My qualifications and professional experience, as well as a list of litigation matters in which I have been engaged as an expert over the past four years, are set forth in my *curriculum vitae*, attached as Appendix B.

8. I have studied telecommunications and systems engineering since approximately 1981 and have over thirty (30) years of industry experience in telecommunications, including wireless communications. During this period, I have also designed and implemented various products involving cellular communication technology.

9. I received a B.S. in Computer and Systems Engineering from Rensselaer Polytechnic Institute in 1985. I received an M.S. in Electrical Engineering in 1988 and a Ph.D. in Electrical Engineering in 1993, both from Stanford University. As a graduate student, I studied the principles of Digital Communications theory, including data modulation and demodulation, signal constellations and lattices, channel estimation, equalization, filtering, precoding, synchronization, and trellis coding. My Ph.D. thesis addressed the application of trellis coding and precoding to a digital modulation system, and was titled “Trellis”

Coding for Multi-Level, Partial Response Continuous Phase Modulation with Precoding.”

10. After receiving my Ph.D. in 1993, I worked for Glenayre Technologies – Wireless Access Group, where I worked on applications for wireless communication, including inventing, designing, and building a patented two-way pager test system and co-developing a wireless application protocol.

11. In January of 1999, I launched a technology consulting company, Protocomm Systems, Inc., which focuses on the development of advanced wireless communications protocols and related software implementations for wireless product companies.

12. From 1999 to 2001, I was also the Director of Software Architecture for Symmetry Communications System. In this position, I was responsible for the software architecture for core SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node) products for the GPRS (Generic Packet Radio Services) market. I also held management responsibility for the Firmware, Hardware, Performance, and Systems Engineering Groups.

13. In 2001, I developed a business plan for building network infrastructure for Institute of Electrical and Electronics Engineers (“IEEE”) 802.11 standard (“Wi-Fi”) enterprise networks, and then later that year founded AirFlow Networks, Inc.

where I invented and received eleven patent son a distributed antenna system design for wireless networks, based on the 802.11 wireless local area network specification.

14. I am currently the Present of Protocomm Systems, LLC and Bims Laboratories, LLC, both of which I founded. As the President of Bims Laboratories, I perform technical research in wireless technology standards, such as UMTS, LTE, 5G, Wi-Fi, Bluetooth, and other network communication protocols. I am named as an inventor on twenty-three telecommunications-related patents.

15. In addition, I am a Technical Expert and former Vice-Chair and Secretary of the IEEE 802.11 Working Group, which develops technical standards for WiFi. Within the IEEE 802.11 Working Group, I routinely participate in discussions relating to the design of wireless communications, including packet prioritization, transmission, acknowledgement, and retransmission.

III. INFORMATION AND MATERIALS CONSIDERED

16. In forming my opinions in this declaration, I relied upon my education and experience in the relevant field of art, and have considered the viewpoint of a POSITA.

17. I have considered the materials referenced herein, including the '552 patent (Ex. 1001), the file history for the '552 patent (Ex. 1003), and other documents listed in the table below:

<u>Exhibit No.</u>	<u>Exhibit Title</u>
Exhibit 1001	U.S. Patent No. 9,961,552, filed May 01, 2018
Exhibit 1003	Prosecution File History for U.S. Patent 9,961,552
Exhibit 1004	WO 2007/086705 (<i>Yun</i>), filed January 26, 2007
Exhibit 1005	US Patent Application Publication 2003/0177267 (<i>Orava</i>), filed
Exhibit 1007	U.S. Patent 8,126,476 (<i>Vardi</i>), filed July 25, 2008
Exhibit 1008	Microsoft Computer Dictionary 5th Edition (Excerpts)
Exhibit 1009	IEEE Std 802.11TM-2012 (<i>IEEE802.11</i>)
Exhibit 1010	US Application Publication 2012/0257536 (Kholaiif), filed
Exhibit 1011	Infringement Contentions for U.S. Patent 9,961,552

IV. LEGAL FRAMEWORK

18. I am not an attorney or a legal expert and offer no opinion on the law. However, I am generally familiar with patentability requests as an inventor on numerous patents and have been informed by counsel of the legal standards that apply with respect to the issues for which I was asked to provide an opinion. I have applied these legal standards in formulating my opinions and arriving at my conclusions. This section summarizes my understanding of the basic legal principles of patent law, as they have been explained to me by counsel.

A. Person of Ordinary Skill in the Art (“POSITA”)

19. I understand that a POSITA is a hypothetical person who is presumed to be aware of all of the relevant art at the time of the invention. I also understand that a POSITA is not an automaton and may be able to fit together the teachings of multiple disclosures, employing ordinary creativity and the common sense that familiar items may have obvious uses in another context or beyond their primary purposes. Further, a POSITA may work as part of a multi-disciplinary team and not only draw upon their own skill, but also take advantage of certain specialized skills of other in the team to solve a given problem.

20. I understand that there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including the education level of active workers in the field at the time of the alleged invention, the sophistication of the technology, the type of problems encountered in the art, and the prior art solutions to those problems.

B. Claim Construction

21. I understand that, in an IPR proceeding, words of a claim are given their plain and ordinary meaning as understood by a POSITA at the time of invention, in light of the specification and prosecution history as well as pertinent evidence extrinsic to the patent.

22. I further understand that statements made by a patent owner during an IPR proceeding, whether before or after an institution decision, may be relevant for

claim construction as they may be relied upon to support a finding of prosecution disclaimer.

23. I understand that, as a general matter, a claim should not be limited to a preferred embodiment, but that in certain cases, the scope may be limited by a narrowing disclosure in the specification or by arguments made or positions taken during patent prosecution or an IPR proceeding.

C. Obviousness

24. I understand that a claimed invention is unpatentable under 35 U.S.C. § 103 if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious to a POSITA to which the subject matter pertains at the time the invention was made. Obviousness, as I understand it, is based on the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and any secondary considerations or objective indicia of non-obviousness to the extent they exist.

25. In analyzing the relevance of the differences between the claimed invention and the prior art, I understand that I must consider the impact, if any, of such differences on the obviousness or non-obviousness of the invention as a whole, not merely some portion of it. The POSITA faced with a problem is able to apply his or her experience and ability to solve the problem and also look to any available prior art to help solve the problem.

26. An invention is obvious if a POSITA, facing the wide range of needs created by developments in the field, would have seen an obvious benefit to the solutions tried by the applicant. When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, it would be obvious to a person of ordinary skill to try the known options. If a technique has been used to improve a process or a device, and a person of ordinary skill in the art would recognize that it would improve similar processes or devices in the same way, using the technique would have been obvious.

27. I understand that I do not need to look for precise teaching in the prior art directed to the subject matter of the claimed invention and I may take into account the inferences and creative steps that a POSITA would have employed in reviewing the prior art at the time of the invention. For example, if the claimed invention combined elements known in the prior art and the combination yielded results that were predictable to a POSITA at the time of the invention, then this evidence would make it more likely that the claim was obvious.

28. On the other hand, if the combination of known elements yielded unexpected or unpredictable results, or if the prior art teaches away from combining the known elements, then this evidence would make it more likely that the claim that successfully combined those elements was not obvious. I further understand that, when prior art discloses multiple options, the teaching away inquiry does not focus

on whether a POSITA would have merely favored one option over another option and the obviousness inquiry does not require that the prior art combination is the “preferred” or “the most desirable” configuration.

29. I further understand that whether there are any relevant differences between the prior art and the claimed invention is to be analyzed from the view of a person of ordinary skill in the art at the time of the invention. I understand that hindsight must not be used to determine obviousness when comparing prior art to the claimed invention.

30. I further understand that obviousness may also be shown if it would have been obvious to combine the teachings of more than one item of prior art. In determining whether a piece of prior art could have been combined with other prior art or with other information within the knowledge of one of ordinary skill in the art, the following are examples of approaches and rationales that may be considered:

- Combining prior art elements according to known methods to yield predictable results;
- Simple substitution of one known element for another to obtain predictable results;
- Use of a known technique to improve similar devices (methods, or products) in the same way;

- Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
- Applying a technique or approach that would have been “obvious to try” (choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success);
- Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; or
- Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

31. I also understand that a suggestion or motivation may come from the knowledge of one of ordinary skill in the art or from explicit statements in the prior art. Alternatively, any need or problem known in the field at the time and addressed by the patent may provide a reason for combining elements of the prior art.

32. I understand that certain objective factors, sometimes known as “secondary considerations,” may also be taken into account in determining whether a claimed invention would or would not have been obvious. For example, certain

secondary considerations, such as independent invention by others within a comparatively short space of time, indicate obviousness.

33. I have been informed by counsel that secondary considerations of non-obviousness which may be raised by a patentee include: (a) commercial success of a product embodying the claimed invention; (b) a long-felt, but unsatisfied need; (c) failure of others to find the solution provided by the claimed invention; (d) deliberate copying by others; (e) unexpected results; (f) praise by others skilled in the art; (g) lack of independent simultaneous invention within a comparatively short space of time; and (h) teaching away in the prior art. I understand that these objective indications are only relevant to obviousness if there is a connection, or nexus, between them and the claimed invention.

34. I also understand that secondary considerations of non-obviousness are inadequate to overcome a strong showing on the primary considerations of obviousness. For example, where the claimed invention represents no more than the predictable use of prior art elements according to their established functions, secondary considerations are inadequate to establish non-obviousness.

V. SUMMARY OF OPINIONS

35. It is my opinion that the claims 1-28 of the '552 patent are rendered obvious by U.S. Patent 8,126,476 ("*Vardi*") (Ex. 1007) in view of IEEE Std

802.11TM-2012 (“*IEEE802.11*”¹) (Ex. 1009), US Patent Application Publication 2003/0177267 (“*Orava*”) (Ex. 1005), and International Publication WO 2007/086705 (“*Yun*”) (Ex. 1004). And it is also my opinion that claims 24-28 of the ’552 patent are rendered obvious by *Vardi*, *IEEE802.11*, *Orava*, *Yun*, and US Application Publication 2012/0257536 (“*Kholaiif*”) (Ex. 1010).

Summary of My Opinions
<i>Vardi</i> , <i>IEEE802.11</i> , <i>Orava</i> and <i>Yun</i> renders obvious claims 1-28
<i>Vardi</i> , <i>IEEE802.11</i> , <i>Orava</i> , <i>Yun</i> , and <i>Kholaiif</i> renders obvious claims 10-28

VI. PERSON OF ORDINARY SKILL IN THE ART

36. It is my opinion that the art of the subject matter of the ’552 patent is telecommunications. After considering several factors, including the types of problems encountered in the field, the sophistication of technology involved, the education background and experience of those actively working in the field, and the level of education that would be necessary to understand the ’552 patent at the relevant time, it is my opinion that the characteristics of a POSITA of the ’552 patent

¹ The abbreviation *IEEE802.11* is used to reference the specific IEEE 802.11

Standard, March 2012 version from prior or subsequent version described as IEEE 802.11, for example, in the prior art references discussed herein.

would have been someone with at least a four-year degree in computer engineering, computer science, or a similar discipline, along with 2 years of professional experience in the fields of networking and network-based systems or applications, or an equivalent level of skill, knowledge, and experience. And would be aware of and generally knowledgeable about how devices were provisioned onto wireless networks, along with standards applicable to well-known methods for communication such as Wi-Fi, Bluetooth, and 3G available at the time the '552 patent was filed. Relevant graduate education could substitute for professional work experience. A POSITA would have had general knowledge of systems and methods used in telecommunication systems and standards, including the solutions and techniques disclosed in the references discussed herein.

VII. TECHNICAL BACKGROUND

37. At a general level, a wireless network is a group of computers and/or associated devices connected by wireless communication devices. For example, a group of computers connected by radio frequency (RF) in a small area can be considered a wireless local area network (“LAN”, and collectively (“WLAN”)). WLAN networks can also be connected to wired networks through, for example, a wireless access point (“AP”). Thus, a wireless network, for example, provided by a coffee shop, can include wireless APs providing access to the Internet.

38. Wireless networks have been around in telecommunications since the 1970s. But, in the past few decades, computer based wireless networks, including Wi-Fi networks, have become pervasive throughout the world. Their use extends to homes, offices, restaurants, airports, and other public establishments. As a result, there have been, and continue to be, efforts to standardize wireless communications to allow interoperability between manufacturers, end devices, users, and network providers in connecting and using the myriad of available networks. Specifically in the computing space, common examples of end user devices can be cell phones, desktop computers, laptop computers, smart devices, personal digital assistants (“PDA”), and other wireless computing devices or devices capable of performing wireless communications, for example, radio communications.

39. A commonly used, well-known standard-based wireless communication network is marketed as Wi-Fi. Wi-Fi is a marketing term used for WLANs that implement the technical standard that is developed and maintained by the 802.11 working group within the Institute of Electrical and Electronics Engineers Standards Association, known as “IEEE 802.11”.

40. As discussed below (*infra* §IX.C), IEEE 802.11 is a well-known standard widely used throughout the industry, and has been published since 1997. Ex. 1009, ix. The standard specifies requirements for wireless communications that

include the definition of the functionality, message formats, and procedures needed to successfully connect to and use WiFi networks.

41. Of relevance to the present proceeding, one aspect of the IEEE 802.11 standard defines how mobile devices connect to and access networks. The principal components of the system are the mobile devices (each identified as a “STA” in the standard), the access point (“AP”) (identified as a “AP-STA” in the standard), and the distribution system (identified as a “DS” in the standard) that interconnects the APs to form the scope of a wireless LAN. The STA obtains access to the wireless LAN through a connection to the AP. According to IEEE 802.11, the STA is not necessarily a device, but instead simply an addressable unit, which can be an origin and/or destination of a frame transmitted across the one or more wireless media. Ex. 1009, 44 (4.2.2 Wireless station (STA)). For example, IEEE 802.11 provides that the station be fixed, portable, or mobile, but the key aspect is that it is an addressable unit for wireless communication. *Id.* Therefore, a wireless user’s end device, such as a cell phone, would include a component, such as, a wireless communication interface that would be the addressable origin or destination of a frame, and thus the addressable unit. And if that component transmitted or received frames for the device, the address of the unit would function as the address for the device.

42. The AP is similarly a device or a component within a device that contains an addressable unit, a STA, and provides access to the distribution services

through wireless medium for stations associated with the AP. *Id.*, 5 (definition of access point). For the purposes of IEEE 802.11, the AP is an AP-STA, which means it also meets the criteria of an addressable unit for wireless communication that is an origin and/or destination of messages. To avoid confusion, the STA will be discussed as the end device or communication device and the AP will be referred to as the computing device providing access to the backbone of the wireless LAN, via distribution services. Accordingly, as stated above, the AP is further connected either wired or wirelessly through these distribution services to other networks, such as, for example, the Internet.

43. As mentioned above, in order for STAs to access a WiFi network, the STA first identifies available APs capable of providing access to the desired network and then associates with the specific AP providing access. A process of identifying and associating with the AP, according to *IEEE802.11*, is illustrated below. As discussed in more detail, the process involves probing by active scanning² (probe

² Probing can also be conducted by passive scanning, wherein the station simply receives transmissions from APs. *Id.*, 979 (10.1.4.2 Passive scanning). Based upon the disclosure and claims of the '552 patent, however, this declaration predominantly focuses on active scanning for the probing/scanning of the IEEE 802.11.

request and probe response), authentication (authentication request and authentication response), and association (association request and association response). In the below figure depicting the sequential communication exchange, the station (STA) is connecting to the network by associating with the access point (AP STA). *Id.*, 84.

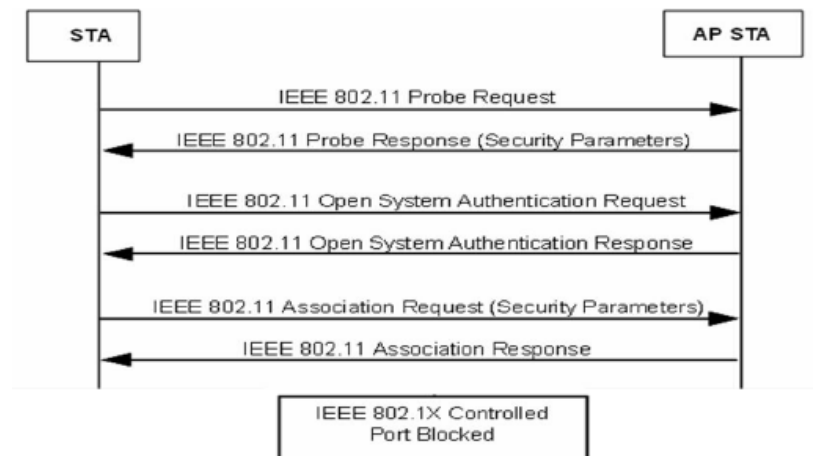


Figure 4-17—Establishing the IEEE 802.11 association

44. In this connection protocol, each transmission from the station to the AP and AP back to the station is formatted and defined by the IEEE 802.11 standard to provide standardization in associating end devices with stations. Thus, manufacturers, users, designers, and network providers can utilize known sets of information from each exchange and can design systems in accordance. Accordingly, the IEEE 802.11 standard sets a format and a minimum amount of information required for the transmissions so devices operating in compliance with

IEEE 802.11 standard can read and use the information in the association process. But the IEEE 802.11 standard sets only a floor, and generally permits additional information to be transmitted by providing additional space for the information in the transmission format.

MAC Frame Format:

45. The transmissions mentioned above are each formatted as frames according to the standard. In other words, for example, according to the standard, the probe request is identified as a probe request frame and corresponds to the format of a probe request frame format. The IEEE 802.11 defines the different types of frame format, which further identifies the required information contained therein. *Id.*, 380 (8. Frame formats). The definition of the frame format is important because of the requirement that the “STA shall be able properly to construct a subset of the frames specified in this clause for transmission and to decode a (potentially different) subset of the frames specified in this clause upon validation following receipt.” *Id.* Thus, by using defined frames according to the standard, stations and APs can exchange communications and understand the communications.

46. The IEEE 802.11 standard is directed to the medium access control (“MAC”) and physical layer of wireless communications, and therefore uses a MAC frame format and a MAC formatted address for the source and destination address for its communications, i.e., a MAC address. *Id.*, Title, 380 (8.2 MAC frame

formats). Each MAC frame includes a MAC header, a frame body corresponding to the specific type of transmission, and a frame check sequence (FCS). A representation of the MAC frame is shown below showing the MAC header, frame body, and FCS. *Id.*, 381 (Fig. 8-1).

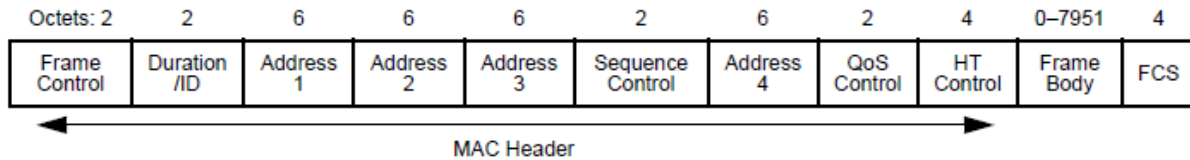


Figure 8-1—MAC frame format

47. The MAC frame format includes the set of fields that occur in a fixed order in all frames, however, only the first three fields (frame control, duration/ID, and Address 1) and the last field (FCS) are necessarily present in all frames. *Id.*, 381. Depending upon the type and subtype of frame certain of the other fields are required, but all of the fields are permitted for all MAC frame transmissions. *Id.*

48. The MAC frame format (MAC header) includes four address fields, which are used to indicate the basic service set identifier (“BSSID”), source address (“SA”), destination address (“DA”), transmitting STA address (“TA”), and receiving station address “(RA)”. *Id.*, 387 (General). As stated above, depending on the particular transmission, not all address fields may be used. *Id.* Each of the above address fields require addresses in the IEEE MAC address format. *Id.*, 387-88 (8.2.4.3.2-8). The multiple address frames can be used, for example, in the scenario where the source or origin of the transmission uses an intermediary station, e.g.,

repeater, booster, etc., to transmit messages. In such a scenario, the source address may be the first station, the destination address may be the final desired address, and the transmitting STA address and receiving STA address may be intermediary station(s) between the source and destination. *Id.*

49. The frame body is defined by type and subtype of the transmission. The above-described transmissions, probe request-response, authentication request-response, and association request-response, are all Management type frames with a subtype corresponding to their name, e.g., probe request, probe response, association request, association response, and authentication. *Id.*, 382-83 (Table 8-1 Annotated Below). The information contained in the frame body functions to conduct the specific instructions associated with the subtype of the transmission.

Table 8-1—Valid type and subtype combinations

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110	Timing Advertisement

Table 8-1—Valid type and subtype combinations (continued)

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication

Connection Protocol:

50. As discussed above, relevant to the present matter is the IEEE 802.11 standard's requirement that a STA must associate with an AP to provide access to, and connect with other networks such as the Internet. As needed, the process begins with identifying available APs to use for connection, authentication between the station and AP, and then association between the station and AP, wherein the station is then connected to the network, and can transmit to and receive information.³

51. A first step in the connection process is considered probing or scanning. The station can operate in either active scanning mode or passive scanning mode. *Id.*, 977. Active scanning, of relevance to the '552 patent, "involves the generation of Probe request frames and the subsequent processing of received Probe Response frames", as shown below in Figure 10-3 (annotated). *Id.*, 977, 980 (Fig. 10-3). The purpose of active scanning is for the station to transmit the probe request frame to trigger proximate available APs to respond and provide certain information for the station to use in selecting to and connecting to the desired AP.

³ The network may have additional restrictions for access, e.g., passwords, but that is beyond the scope of IEEE 802.11 standard.

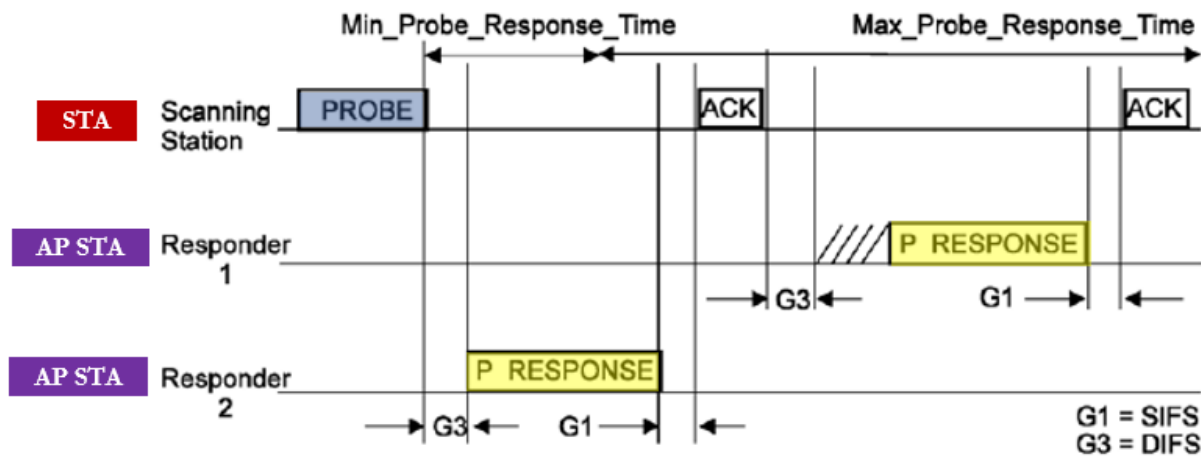


Figure 10-3—Probe response

52. The probe request frame is in the MAC frame format and includes the MAC header, as noted above. Thus, the probe request frame includes a MAC address of the station. IEEE 802.11 is not specific enough to require the MAC address included in the probe request frame be the actual MAC address, but only that the address provided therein be in the IEEE 802 MAC address format. *Id.*, 387-88. For example, the Address 1 field of the MAC header can be the specific MAC address of the station and Address field 3 can be the BSSID of the station, both of which would be in the IEEE 802 MAC address format. *Id.*, 979.

53. In response to receiving a probe request, an AP responds by transmitting a probe response frame, which is a management type probe response subtype transmission. *Id.*, 84 (Fig. 4-17). The purpose of the probe response frame is to provide sufficient information to the station for the station to begin the authentication and association procedures with a desired AP. As such, the probe

response frame includes the service set identified (SSID), i.e., the name of the network the AP is providing access, and the BSSID, which is an IEEE 802 MAC address of the AP, as shown below in Table 8-27 showing the probe response frame body. *Id.*, 430-32 (providing the frame body of management frame of subtype probe response).

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 8.4.2.2.
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set element is present within Probe Response frames generated by STAs using FH PHYs.

.

.

.

Order	Information	Notes
23	Measurement Pilot Transmission	The Measurement Pilot Transmission element is present if dot11RMMeasurementPilotActivated is between 2 and 7.
24	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RMMeasurementPilotActivated is between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 10.11.14) with two or more members, or if dot11MgmtOptionMultiBSSIDActivated is true, or if dot11InterworkingServiceActivated is true and the AP is a member of a Multiple BSSID Set with two or more members and at least one dot11GASAdvertisementID MIB attribute exists.

54. After the station receives and processes the probe response frame from the AP (*id.*, 978), the IEEE 802.11 connection protocol proceeds to the authentication phase, as shown below. *Id.*, 84 (Fig. 4-17).

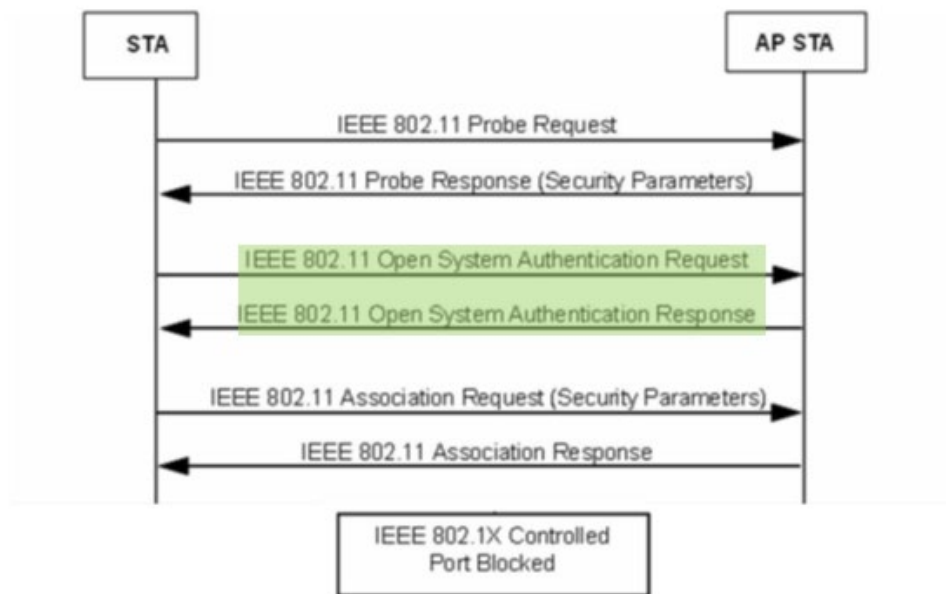


Figure 4-17—Establishing the IEEE 802.11 association

55. As demonstrated by the arrows, IEEE 802.11 authentication includes the station sending an authentication request and the AP responding by sending an authentication response. *Id.*, 1014-15 (10.3.4.2 Authentication—originating STA, 10.3.4.3 Authentication—destination STA). The authentication transmissions are management type authentication subtype frames, including the MAC header and subtype Authentication frame body. *Id.*, 380-83. Within the context of the IEEE 802.11 standard, the purpose of authentication is “to establish the identity of one station (STA) as a member of the set of STAs authorized to associate with another STA.” *Id.*, 6 (definition of authentication). Thus, authentication in this context is a required pre-requisite to association, as only authorized STAs can associate with

another STA, such as an AP, and includes the exchange of authentication request and authentication response frames.

56. The final relevant phase of establishing an IEEE 802.11 standard connection is the association phase, which comprises the exchange of an association request frame, and an association response frame, which are both management type frames and individually association request and association response subtype frames. *Id.* The station transmits an association request frame to the AP (*id.*, 1016-17 (10.3.5.2 Non-AP STA association initiation procedures), and the AP receives and evaluates the association request frame and then transmits an association response frame (*id.*, 1017-19 (10.3.5.3 AP association receipt procedures). Shown below in Fig. 4-17 (annotated) is the association request-response phase, concluding the IEEE 802.11 connection establishment procedure. Within the context of the IEEE 802.11 standard, the purpose of association is “to establish access point/station (AP/STA) mapping and enable STA invocation of the distribution system services (DSSs).” *Id.*, 6 (definition of association). This means that, once associated, a mobile device can access the Internet through a nearby access point. This is because an association service (which includes the exchange of association request and response frames) informs the IEEE 802.11 distribution system (DS) about the mapping between a mobile device and an access point.

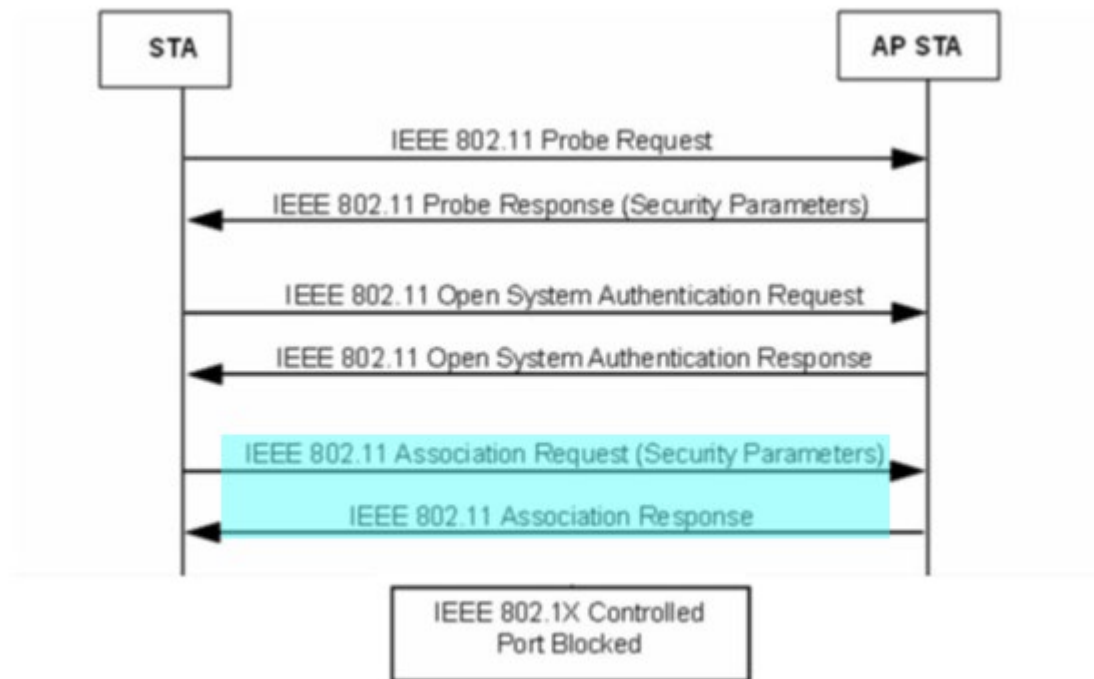


Figure 4-17—Establishing the IEEE 802.11 association

57. Successful association concludes the IEEE 802.11 standard connection establishment and provides access to the network through the AP and the exchange of information between station and network. *Id.*, 1016 (“Successful association enables a STA to exchange Class 3 frames. Successful association sets the STA’s state to State 3 or State 4.”). At this point, the network may have additional access hurdles, but the station is connected to the network through the AP as provided by IEEE 802.11 standard.

VIII. THE ’552 PATENT

58. The application that issued as the ’552 patent was filed on April 22, 2015, and is a continuation of application Ser. No. 13/885,754, filed May 16, 2013,

now U.S. Pat. No. 9,717,005, which is a U.S. Natl. Stage filing of International Appl. No. PCT/US12/66306.

A. The Subject Matter Described

59. The '552 patent describes methods and devices for secured wireless network communications, generally between an end device, and a network through a wireless AP. *See* Ex. 1001, 2:64-67. Generally, the end device (130) and the method (300) described are shown in Figs. 3 and 4, reproduced below. *Id.*, Figs. 3-4.

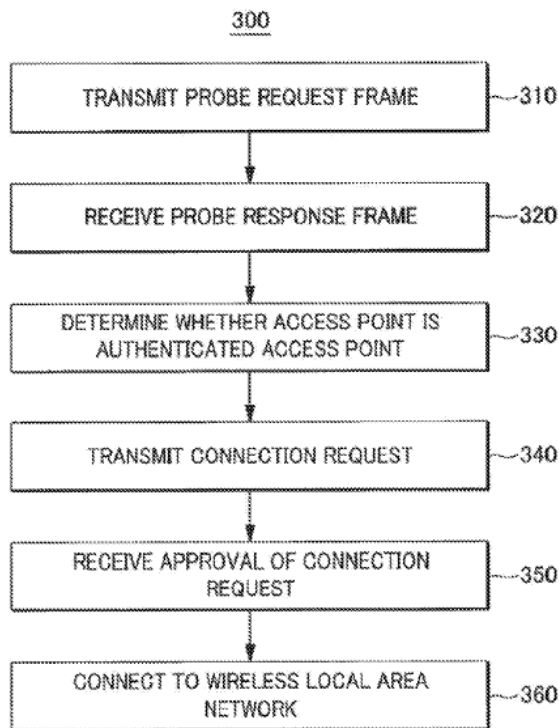


FIG. 3

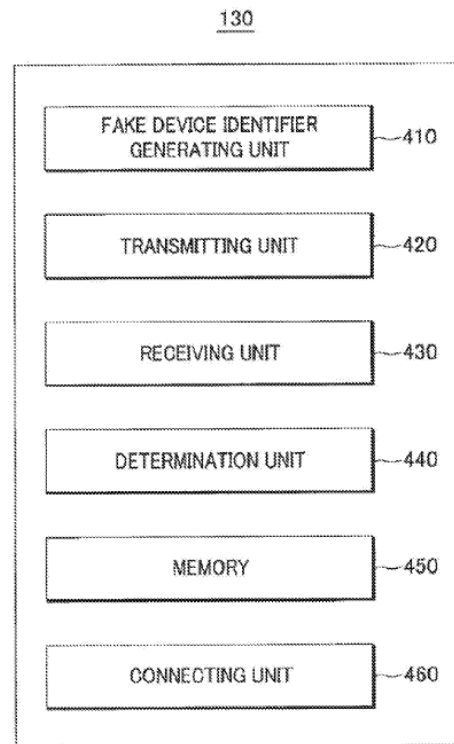


FIG. 4

60. The procedure described in the '552 patent (reproduced and annotated below -- left) aligns with the connection procedure defined in *IEEE802.11*

(reproduced and annotated below -- right). Compare Ex. 1001, Fig. 3 with Ex. 1009, 182 (Fig. 4-17). As shown below, each procedure step except (330) correlates explicitly to a procedure step defined by *IEEE802.11*'s connection procedures, which are annotated to represent similar procedure steps.

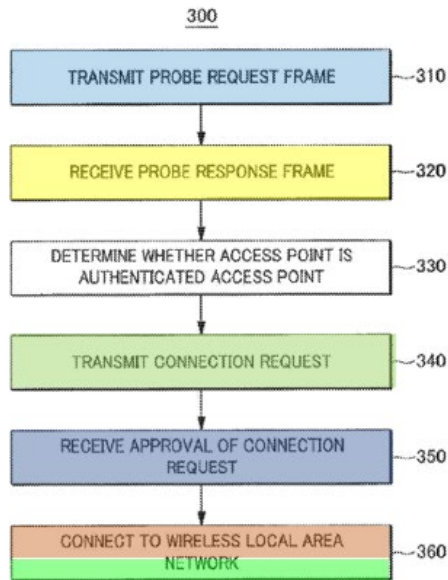


FIG. 3

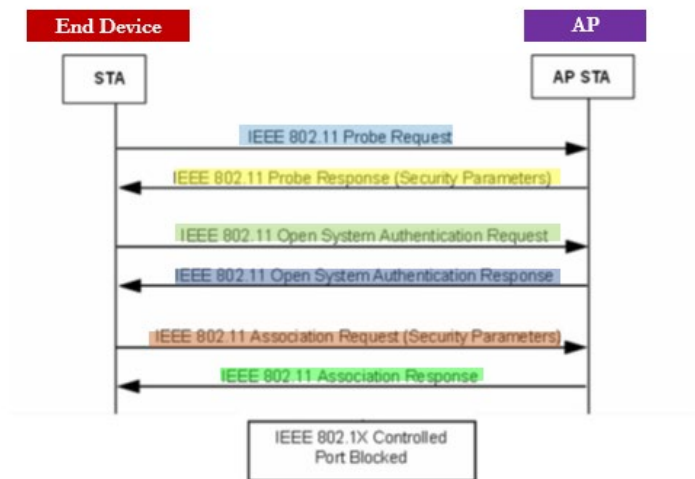


Figure 4-17—Establishing the IEEE 802.11 association

61. According to the '552 patent, connecting to a wireless network begins with the end device transmitting a probe request frame (310) to all proximal APs. Ex. 1001, 3:4-12, 5:12-15; *see also* Ex. 1009, 182 (Fig. 4-17) (Probe Request). The '384 patent describes that in the prior art, the probe request frames included an authentic MAC address, which is permanent and unique, for the end device. *Id.*, 3:10-12. However, use of the authentic MAC address in the public probe request, could expose the present location information of the device to undesired APs. *Id.*, 3:12-18.

62. To prevent such undesired disclosure, the '552 patent has the end device generate and transmit a fake device identifier, *e.g.*, fake MAC address, instead of the permanent (authentic) device identifier, permanent (authentic) MAC address, in the probe request frame. Ex. 1001, 3:19-22, 3:65-4:10, 5:12-15.

63. After transmitting probe request frame (310), the end device receives one or more probe response frames (320), as also shown in *IEEE802.11. Id.*, 3:22-24, 5:19-21; *see also* Ex. 1009, 182 (Fig. 4-17) (Probe Response). The probe responses frames include access point information ("API") of the respective AP, including their MAC address and/or service set identified ("SSID"). Ex. 1001, 4:13-17, 5:21-26.

64. The '552 patent describes different methods to determine a preferred AP, or authenticated AP ("AAP"), based on the API received in the probe response frame (330). *Id.*, 3:29-32, 4:18-36, 5:27-45. One methodology includes comparing received API to an authenticated AP list ("AAPL"), for example, by determining whether the received API (*e.g.*, MAC address and/or SSID) is included in the AAPL. *Id.* The AAPL may contain a list of AAPs that include APs controlled by a server or APs previously connected with the end device. *Id.* Alternatively, an AAP can be determined by determining whether an AP was previously connected with the end device or controlled by the server based, at least in part, on the API in the probe response. *Id.*

65. The end device then transmits a connection request—a non-defined phrase in the IEEE 802.11 standard—which can include an authentication request, to the AP selected for connection (340), including the authentic device identifier of the end device. *Id.*, 4:46-48, 4:51-55, 5:46-53; *see also* Ex. 1009, 182 (Fig. 4-17) (Authentication Request).

66. In response, as shown by *IEEE802.11*, the end device receives a connection approval response (350)—a non-defined phrase in the IEEE 802.11 standard—which can include an authentication response. *Id.*, 4:56-59, 5:54-57; *see also* Ex. 1009, 182 (Fig. 4-17) (Authentication Response).

67. Following this, the end device obtains access to the wireless local area network (“WLAN”). Ex. 1001, 5:58-60. This includes an association process with the AP through the exchange of association request and response frames (360). Ex. 1001, 4:60-64; *see also* Ex. 1009, 84 (Fig. 4-17) (Association Request-Response). Following the receipt of the association response, the end device is connected to the network. Ex. 1001, 4:64-65.

68. A device configured to perform the above-described method is also described, as shown in Figures 1 and 4 (reproduced below). Figure 1 illustrates a system including end device (130) in network area (140) provided by AP (120). Ex. 1001, 3:45-52, Fig. 1. As further shown in Figure 4, end device 130 may include

generic components to facilitate the above-described method. *Id.*, 6:5-11, Fig. 4.

Notably, no algorithms or specialized components are described in the '552 patent.

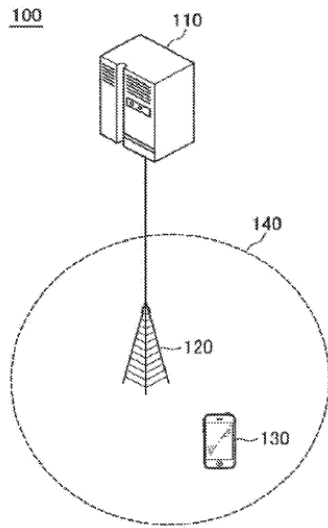


FIG. 1

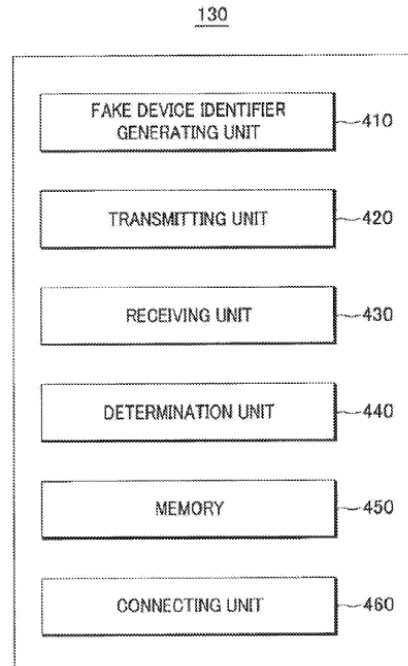


FIG. 4

B. The Prosecution History

69. The application that issued as the '552 patent was filed on April 22, 2015, and is a continuation of application Ser. No. 13/885,754, filed May 16, 2013, now U.S. Pat. No. 9,717,005, which is a U.S. Natl. Stage filing of International Appl. No. PCT/US12/66306.

IX. OVERVIEW OF THE PRIOR ART REFERENCES

A. Vardi

70. *Vardi* describes a system and method for mobile devices, identified as user terminals (“UT”) or clients, to connect to APs in conjunction with a server

stored database. Ex. 1007, 3:4-6, 4:18-25, 4:43-57. *Vardi* discloses server containing a database of APs and stores and collates information corresponding to APs for its “clients” (i.e., UTs) to utilize in real time. *Id.*, 7:10-20, 7:33-36. The information stored and collected is based on prior connections between clients and APs and includes API, for example, the MAC address and SSID of the previously connected APs. *Id.*, 3:21-30, 11:41-42. Clients continuously update the server based on their interaction and connection with APs. *Id.*, 3:4-6, 4:18-25, 8:7-21. The server then updates its database and sends corresponding updates about relevant APs to its clients. *Id.* To obtain information about APs, *Vardi* discloses utilizing an IEEE 802.11 scan to identify active and available APs and obtain API. *Id.*, 10:34-36, 11:35-36, 13:4-7, 14:52-57. The client compares the API obtained from available APs to the API in the database to determine which AP to connect to, including based upon previous connections. *Id.* Once the preferred AP is selected the mobile device connects with the AP according to IEEE 802.11. *Id.*

71. *Vardi*’s system and method is built on what *Vardi* confirms was known in the art:

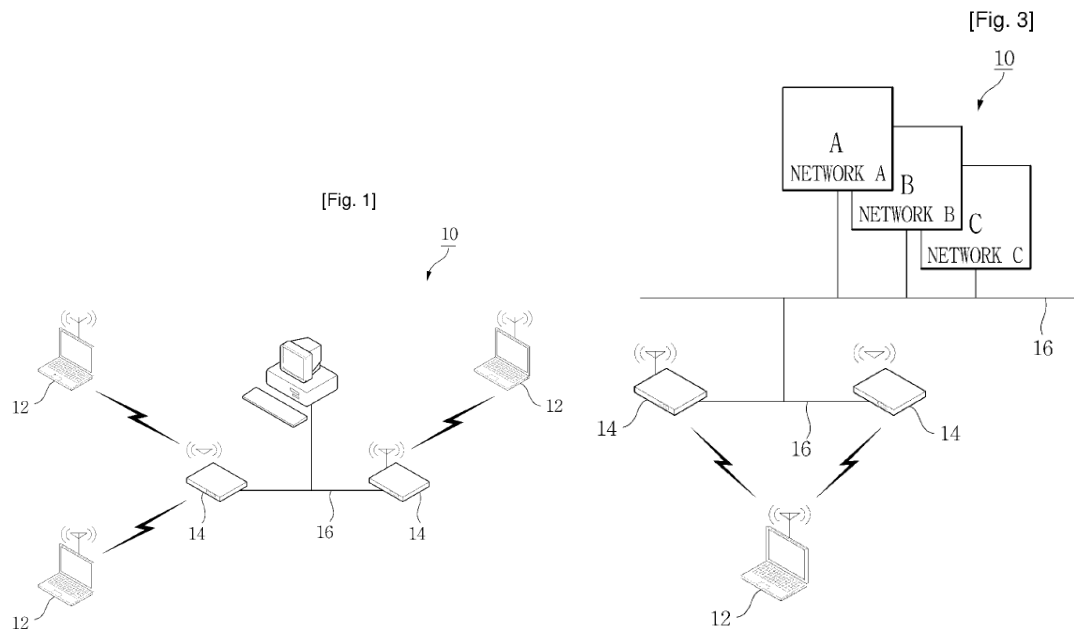
[I]t is well known in prior art computing systems to cache information related to an access point to which the mobile device has connected before. In this manner, when the mobile device is activated at a later time in the same locale, the system uses the information in the cache to automatically

reconnected to that AP. The cache normally includes the name and the MAC address of the AP. Ex. 1007, 12:24-30.

72. The prior art recognized storing MAC addresses and SSIDs (e.g., name) of previously connected to APs was beneficial to the connection process. Specifically, by storing this information, *Vardi* teaches the second time a user terminal comes across the MAC address or SSID of the previously connected AP, for example by active or passive scanning, it can compare that MAC address or SSID to the stored list of previously connected to APs and, if matched, select that AP for automatic connection. *Id.*

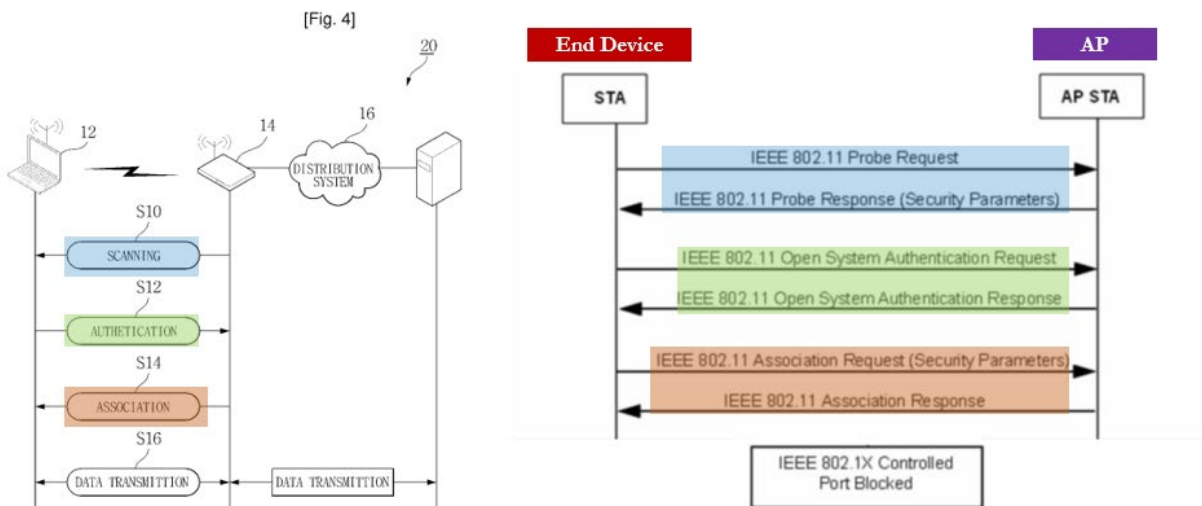
B. Yun

73. *Yun* describes a wireless network system and communication methods for wireless networks. Ex. 1004, (54).



74. Figures 1 and 3 of *Yun* (reproduced above) illustrate two embodiments of *Yun*'s wireless network system. The system includes stations(12) connected to WLANs(10) through APs(14) and distribution system(16). *Id.*, ¶[17], ¶[20], ¶[22], ¶[25]. The stations include network interface cards (NIC) to connect to the WLAN in accordance with IEEE 802.11 standard. *Id.*, ¶[17].

75. Figures 4 and 5 (reproduced and annotated below) illustrate the connection process for securely connecting the station to the WLAN, which corresponds to the connection process defined in *IEEE802.11*, which are annotated in color to indicate corresponding steps. *Id.*, Fig. 4, Ex. 1009, 84 (Fig. 4-17).



76. Scanning(S10) by the station includes active scanning to identify available APs by broadcasting probe requests to available APs. Ex. 1004, ¶[31]-[32]. In response, the station receives probe responses from the APs including API such as SSID. *Id.*, ¶[32].

77. In order to provide MAC address anonymity during probe requests frame exchanges, *Yun* describes using an arbitrary MAC address, identified as AMID or Dynamic MAC address, instead of the actual MAC address. *Id.*, ¶¶[144]-[146], ¶¶[154]-[156]. The station generates the arbitrary MAC address and then transmits a probe request frame including the arbitrary MAC address to the AP instead of the actual MAC address of the station. *Id.*, ¶[146], ¶¶[154]-[156].

78. After scanning is complete, the authentication process(S12) occurs which includes performing Open-system authentication according to IEEE 802.11, including the station transmitting an authentication request to the AP and receiving an authentication response. *Id.*, ¶[35]. An association process(S14) follows to associate the AP with the station and provide access to the WLANs. Ex. 1004, ¶¶[36]-[38].

C. IEEE802.11

79. *IEEE802.11* was published as a standard by the Institute of Electrical and Electronics Engineers (“IEEE”) in March 2012. The 2012 edition “gives users, in one document, the *IEEE802.11* standard for wireless local area networks (WLANs) with all the amendments that have been published to date.” Ex. 1009, ix. By early 2012, *IEEE802.11* was publicly available, well-known, and widely available to (and considered by) POSITAs. At the time of its publication and afterwards, *IEEE802.11* was a well-known standard in the wireless industry

specifying aspects of wireless local area networks (“LAN”); *Id.*, 1782 n.51 (“IEEE publications are available from The Institute of Electrical and Electronics Engineers (<http://www.standards.ieee.org/>).”).

80. *IEEE802.11* specifies “[t]he medium access control (MAC) and physical characteristics for wireless local area networks (LANs).” *Id.*, iii. It describes the process by which mobile devices join and communicate with other stations. *Id.*, 978. Specifically, the mobile device can use “Active scanning[, which] involves the generation of Probe frames and the subsequent processing of received Probe Response frames.” *Id.*, 978.

81. A typical probe request frame exchange seeks a response from *any* BSS and does not include the address of a specific SSID. *Id.*, 126. This is shown, in part, in Figure 10-3, which shows the scanning station issuing a probe request frame, and responder stations 1 and 2 transmitting probe response frames:

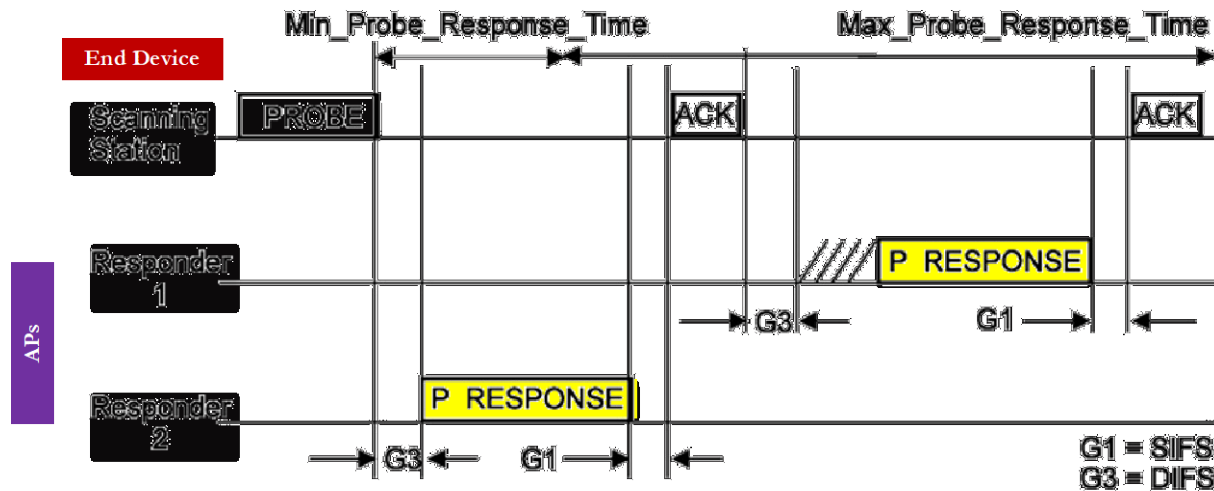


Figure 10-3—Probe response

82. If a device wishes to probe a specific BSS, for example a previously connected AP, then it appends to the probe request frame the SSID of the specifically-targeted BSS during the active scanning process. *Id.*, 126. Generally speaking, stations “receiving Probe Request frames shall respond with a probe response only if” the SSID in the probe request is the broadcast SSID or matches the specific SSID of the STA.” *Id.*, 979.

D. Orava

83. *Orava* discloses a system comprising “a terminal device MT and a WLAN network according to any version of the *IEEE802.11* standard.” *Id.*, ¶[19]. *Orava*, however, recognized that the use of fixed MAC addresses in IEEE 802.11 messages posed “a security risk: a MAC address can be picked up from every message transferred over the air interface... When the MAC address of the device is

known, the movements of the device can be followed, and its traffic can be deliberately disturbed by causing collisions with packets by using a ‘stolen’ MAC address.” Ex. 1005, ¶[3]. And *Orava*’s disclosures sought to put POSITAs on notice and teach them how to overcome this risk.

84. Thus, *Orava* provides procedures for generating and transmitting a random MAC address maintaining compliance with the 802.11 standard. Ex. 1005, ¶[49]. It discloses the use of a random MAC address to facilitate a connection by a mobile terminal (“MT”) through an access point. Ex. 1005, ¶[22].

85. But *Orava* also recognizes that it may only be advantageous to remain anonymous during the arrangement stage—during scanning—between the MT and AP. *Id.*, ¶[25]. Not only does *Orava* provides a POSITA with numerous methods for generating an IEEE complaint random MAC address, *Id.*, ¶[30]. *Orava*, further, explains utilizing the random MAC address in the pertinent IEEE 802.11-based connection procedures, including scanning (active and passive), authentication, association, and subsequent connection to wireless devices. *Id.*, ¶¶[20], [29]-[31], and [49].

E. Kholaiif

86. *Kholaiif* discloses configuring mobile stations for WLAN deployment. *Kholaiif* explains that the “various techniques disclosed in this document are... in the context of IEEE 802.11-based wireless networking. This context is described in the

IEEE 802.11 specifications for wireless local area network (WLAN) media access control (MAC) and Physical Layer (PHY).” Ex. 1010, ¶[2].

87. And FIG. 27 provides “a functional block diagram illustration of an example mobile station.” Ex. 1010, ¶[37].

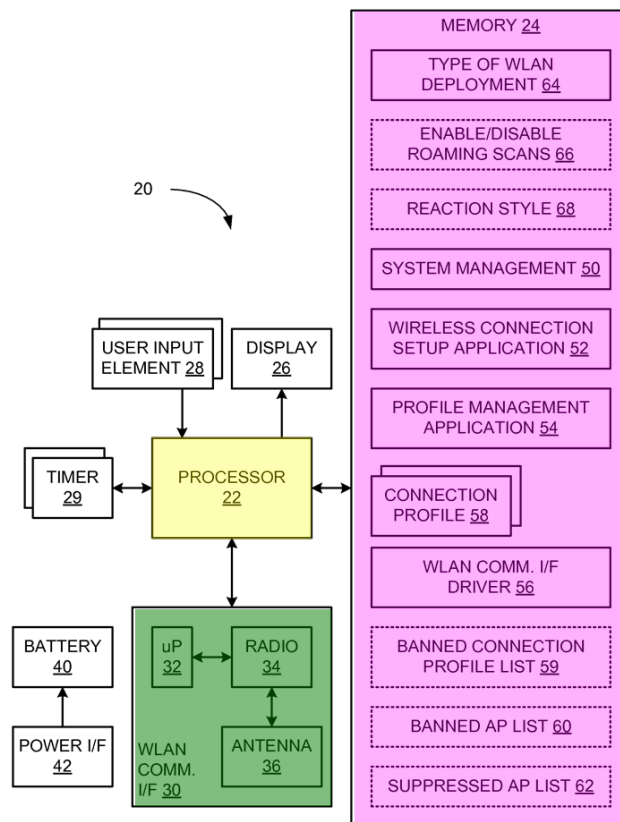


FIG. 27

F. Motivation to Combine

1. Vardi, IEEE802.11, Orava, and Yun

88. In my opinion, it would have been obvious to a POSITA to combine the teachings of *Vardi, IEEE802.11, Orava* and *Yun* to achieve the methods and

systems described by *Vardi* and incorporating the underlying implementation of the IEEE 802.11 Std. transmissions described by *Vardi* with *IEEE802.11*'s explicit teachings and further improving the security of *IEEE802.11*-based probe request frames taught by *Vardi* by incorporating the security improvement of substituting a randomly generated MAC address as taught by *Orava* for the actual MAC address of *Vardi* into the probe request frame as taught by *Yun* to prevent MAC address disclosure and identification of the mobile device by devices receiving the probe request frame.

89. In short, but not exclusively, *IEEE802.11* provides underlying implementation details to the methods and systems disclosed by *Vardi*, *Orava*, and *Yun*. While *Orava* and *Yun* provide security control management to protect the mobile device's "real" MAC address.

90. *Vardi* teaches or at least suggests all the claimed 802.11 connection procedure steps and components to perform those steps between a mobile device and access point (AP)—probing, authentication, and association.

91. To the extent that its description uses only well-known terms of art, for example, "scan" or "probing," a POSITA would have known these terms have meanings as defined by *IEEE802.11*.

92. Although *Vardi* does not detail the underlying implementation of, for example, performing an "IEEE 802.11 scan," "probing," or "IEEE 802.11

association,” *Vardi* does explicitly disclose using *IEEE802.11* to connect a mobile device and AP.

93. Therefore, a POSITA would naturally look to *IEEE802.11* to fill any alleged gaps.

94. It would have been obvious to a POSITA to apply the *IEEE802.11* to provide the underlying details of *Vardi*’s “IEEE 802.11 scan,” “probing,” or “IEEE 802.11 association.”

95. Moreover, not only would it have been expected of a POSITA to become familiar with the standard as part of their work experience because the standard underpinned the development of most commercial equipment, *Vardi*, *Orava*, and *Yun* explicitly direct a POSITA to the standard to implement the disclosed systems and methods. Ex. 1007, 7:36-43; Ex. 1005, ¶[19]; Ex. 1004, ¶[230].

96. *Vardi* alone discloses the well-known components required by claims 24-28.

97. Specifically, *Vardi* discloses that a “user terminal can be a device that executes a program... to find usable radio resources or wireless APs,” “clients can continuously collect radio resource information about AP’s [sic] detected by the wireless terminal. These clients can be executed on laptops, handheld[] devices (PDA[s]), cellphones, or other devices that incorporate radio facility for wireless

communication, such as WiFi,” a POSITA would understand this disclosure satisfies the claimed processor and communication interface including a transmitter and receiver. Ex. 1007, 7:10-14, 9:54-59.

98. *Vardi* discloses that “user’s clients can store... information in the memory of the wireless user terminal” and “can compare [received] scan result with its radio resource database to determine which APs are preferred for connection and roaming.” Ex. 1007, 7:31-32, 14:55-57.

99. A POSITA would have readily understood these disclosures as satisfying the claimed “memory” and “determination unit” components of the claims.

100. *Vardi*, however, does not disclose using a Fake ID. But what *Vardi* lacks—randomly generated Fake ID—is disclosed by *Orava* and *Yun*.

101. It would have been obvious to a POSITA to apply *Orava*’s randomly generated Fake ID and *Yun*’s anonymous probe request frame exchange transmission while remaining *IEEE802.11* compliant to the *Vardi* system.

102. Even though, in my opinion, *Vardi*’s hardware disclosure is taught or at least obvious to a POSITA, *Orava* is explicit.

103. It would have been obvious to a POSITA to implement *Vardi*’s system utilizing these well-known components of *Orava*.

104. Between *Vardi*, *Orava*, and *Yun*, they reference *IEEE802.11* more than fifty times. *Vardi*, *Orava*, and *Yun* provide a POSITA with a roadmap to implement their teachings as *IEEE802.11* compliant and compatible systems.

105. To ensure proper formatting of the probe request/response frames that *Vardi*, *Orava*, and *Yun* disclose, a POSITA would have turned to the *IEEE802.11* specification, which defines the probe request and probe response frame format.

106. *Vardi*, *IEEE802.11* *Orava*, *Yun*, and the '552 patent are all analogous art because they are directed to the same field of wireless communication using the IEEE 802.11 standard. See '552 patent, Abstract, 7:45-46; *Orava*, Abstract; Ex. 1007, Abstract, 7:36-38; Ex. 1004, ¶[230].

107. *Orava* starts with *IEEE802.11*, identifies a problem, and seeks to solve the problem with a clear and explicit solution that remains *IEEE802.11* compliant. Ex. 1005, ¶¶[30], [49].

108. A POSITA would have been particularly motivated to look to *Orava*'s teachings to improve the *Vardi* communication system because *Orava* described the problem with *Vardi* using manufacturer-assigned fixed MAC addresses.

109. Specifically, *Orava* informed a POSITA that “the fixed MAC address determined by manufacturers cause a security risk: a MAC address can be picked up from every message transferred over the air interface...” Ex. 1005, ¶[3].

110. *Orava* also detailed the solution, “[i]n order to arrange anonymity, it has been suggested that temporary random MAC addresses be used for WLAN networks.” Ex. 1005, ¶[4]; see also Ex. 1005, ¶[29].

111. *Orava* provided numerous solutions for generating random fake identifiers, it did so using the *IEEE802.11* roadmap. Ex. 1005, ¶[30] (“The IEEE 802 MAC address format allows locally administrable MAC address, in which there are 46 available bits in a 48-bit address format for selecting the temporary MAC address.”) enabling a POSITA to maintain standard compliance.

112. There were well-known benefits of using fake identifiers when establishing wireless communications.

113. Wireless communications (e.g., Wi-Fi, 3G, 4G) that send messages over radio waves may be intercepted by unauthorized third parties. Encrypted communications ensure that only an authorized receiver can view the contents of the messages. User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting their availability for a device to connect to their network.

114. As *Yun* teaches, enabling Wi-Fi connectivity to use a fake identifier before the connection phase with an access point before sharing the user’s private identifier would have prevented third-party attackers or unauthorized third parties from compiling a list of SSIDs and private location information based on previously used hotspots.

115. Specifically, *Yun* teaches “MAC address anonymity makes an identity of the station not presumed through the MAC address... The transmitted packet on air uses an arbitrary MAC address(‘Dynamic MAC address’)... [the] invention relates to what protects the real MAC address of the station... the station transmits the ... MAC address request such as the probe request.” Ex. 1004, ¶¶[154-156].

116. The IEEE 802.11 standard is the foundation of *Vardi*’s, *Orava*’s, and *Yun*’s teachings.

117. For example, each utilize the IEEE 802.11 Active Scan procedure comprising of transmitting probe-request-response frames. Ex. 1007, 10:34-36 (“Basic IEEE 802.11 association procedure. . . using ... probing to get association information”), 7:36-40; Ex. 1005, ¶¶[29] (“the terminal MT transmits a Probe request”), ¶[49] (“temporary MAC address can thus be used... in all protocol messages.”); Ex. 1004, ¶[156] (“the station transmits the data including the MAC address request such as the probe request(‘Dynamic MAC address Request’) to the access point.

118. Because each system shares a foundational standard, it ensures interoperability between *Vardi*, *Orava*, and *Yun* for a POSITA with minimum effort and no undue experimentation.

119. A POSITA would have a reasonable expectation of success in applying *Orava*’s temporary MAC address teachings with transmitting in *Yun*’s probe request

into *Vardi*'s wireless communication system because *Vardi*'s system already exchanges probe request and response frames that include a MAC address as defined and taught by *IEEE802.11*.

120. A POSITA merely exchanges the probe request frame's real MAC address (also randomly generated by the manufacturer) for a temporarily generated random MAC address (Fake ID) to maintain interoperability.

121. Configuring *Vardi*'s wireless system to substitute the "real" MAC address for *Orava*'s temporary MAC address would have been a straightforward and routine application of well-known techniques in wireless communications. This straightforward and routine application is apparent because:

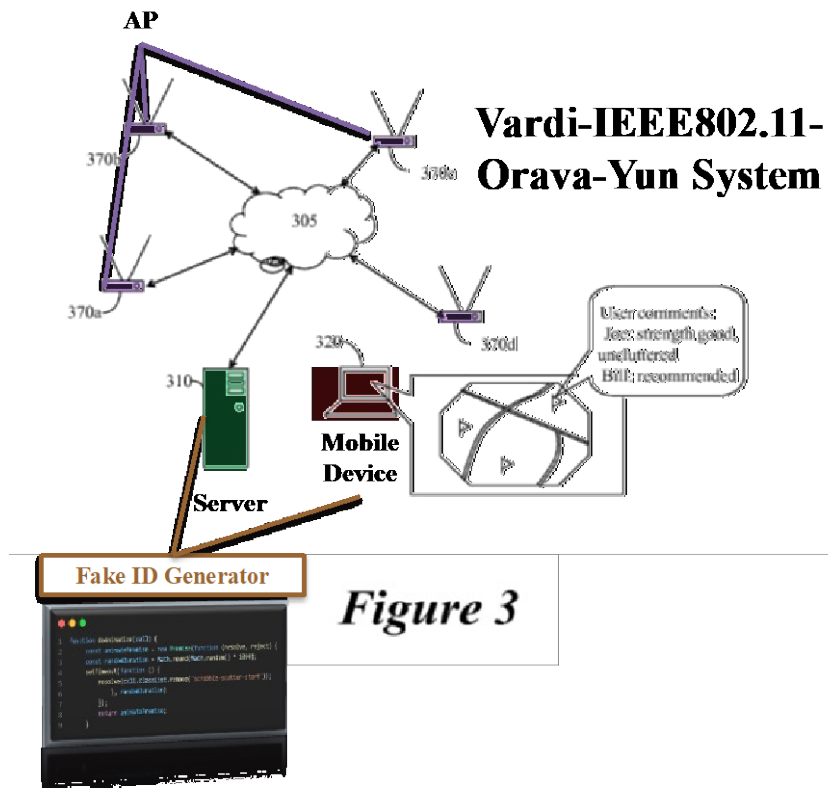
- MAC addresses are themselves randomly generated per manufacturer, and thus randomly generating MAC addresses was well-known in the art;
- *Vardi*'s mobile device and server includes a processor and software to execute the random generation software;
- it merely requires generating or receiving a random number or letter, plugging it into the standard IEEE 802.11 probe request frame without any modification to the standard or frame format;
- *Vardi*'s server and mobile device are already configured to transmit data;
- *Vardi* transmits probing messages to APs per *IEEE802.11* standard; and

- a POSITA would have been capable of implementing a temporary identifier within the existing system.

Ex. 1007, 7:59-60; Ex. 1005, ¶¶[3], [49]; Ex. 1004, ¶¶[154-156].

122. In summary, *Vardi*, *Orava*, and *Yun* specify the use of *IEEE802.11* and assume a POSITA was familiar with implementing and modifying a WLAN network at least because each *Vardi*, *Orava*, and *Yun* explicitly recite “IEEE 802.11.” Thus, a POSITA would have naturally turned to the *IEEE802.11* standard for implementation details.

123. At the same time, both *Orava* and *Yun* provide the random MAC address generation functionality to minimize location tracking in the *Vardi* communication system and method (“*Vardi-IEEE802.11-Orava-Yun*”).



G. Motivation to Combine

1. Vardi, IEEE802.11, Orava, Yun, and Kholaiif

124. The *Vardi-IEEE802.11-Orava-Yun* system renders obvious claims 1-28. Despite the explicit disclosures above regarding well-known components of mobile devices at the time of the alleged invention, the PO may contend that the references do not disclose the connections between the components or within the mobile device. But *Kholaiif* does. *Kholaiif*, FIG. 27.

125. *Kholaiif* explicitly discloses each of the well-known components recited by claims 24-28. *Kholaiif*, FIG. 27. A POSITA would have looked to and for

components that support IEEE 802.11 standard communications when deploying mobile devices in an IEEE 802.11 WLAN.

126. A POSITA would naturally look to *Kholaif* for those disclosures, particularly here, where *Kholaif* also discloses selecting a target access point based on the results of a discovery scan procedure, the type of network to which the access point provides access. *Kholaif*, Abs., [52], [56], Fig. 2. The information used to select the desired access point includes the SSID. *Id.* at [90], [120]. *Kholaif* further teaches an authentication procedure, including associating the mobile station with the target AP. *Id.* at Fig. 2, [49], [51], [59], [64], [65], [69]. *Kholaif* discloses the use of these techniques in the context of IEEE 802.11—based wireless networking. *Id.* at [2], [38]. *Kholaif* also discloses a mobile station that can authenticate access points based on information about the access points, which includes a processor and a memory. *Id.* at [197], [242], [245].

127. Like *Vardi*, *IEEE802.11*, *Orava*, and *Yun*, *Kholaif* is also in the same field of endeavor as these references and to the '552 patent.

128. The proposed combination would have been nothing more than (1) using known components, (2) inside known devices, (3) for their known purpose, (4) implementing a known standard for WLAN communication—the same *IEEE802.11* standard.

129. A POSITA would have a reasonable expectation of success because using standardized supported components would have been common and expected. Moreover, as explained above, *Vardi* and *Orava* disclose the same components and instructs a POSITA that the components need to be operable with *IEEE802.11*.

130. In summary, although a POSITA would have known that *Vardi*'s "clients [] execut[ing] on laptops, handheld devices, PDA's, cellphones, and other device[s] that incorporates a radio facility for wireless communication, such as Wifi," disclose the well-known components of claims 8-13; nonetheless, *Kholaif* illustrative discloses those components, and it would have been obvious to a POSITA to ensure these well-known components were implemented and would have done so, successfully.

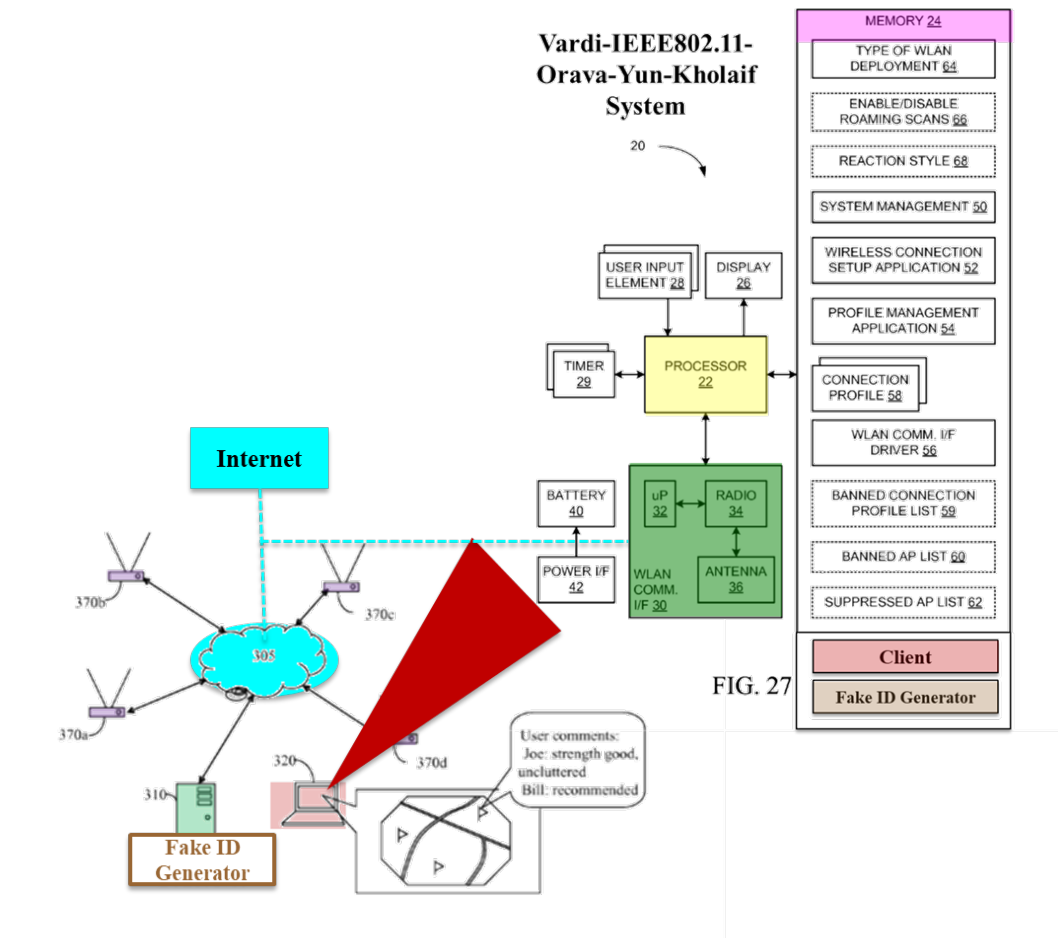


Figure 3

X. VARDI, IEEE802.11, ORAVA AND YUNRENDER CLAIMS 1-9 OBVIOUS

A. Obviousness of Claims 1-9 (IPR2024-01368 Ground 1)

131. In my opinion *Vardi*, *IEEE802.11*, *Orava*, and *Yun* renders obvious claims 1-9.

1. Independent Claim 1

132. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 1.

i. Limitation 1[pre]:

1[pre] A method performed by a server, the method comprising:

133. I understand that the preamble of claim 1 merely states the purpose or intended use of the claimed subject matter, which is not limiting.

134. In my opinion, *Vardi* teaches the preamble.

135. *Vardi* teaches a wireless communication system including a server, a mobile device, and an access point. Where the server performs a method of transmitting access point (“AP”) information (“API”) to mobile devices to assist in connection to the Internet between the mobile devices and APs. Ex. 1007, 3:4-6 (“According to the invention, clients receive updates about relevant access points from the server and use the information to select and connect to the preferred access point.”), 13-24 (“The method can include receiving a first set of data from a user terminal about radio resources (wireless access points) in reach of the user terminal and storing the information about each access point in one or more databases. . . . Once information about an access point is stored in the database(s), it can be sent to one or more user terminals and used by each user terminal to select a preferred radio resource for connection.”), 3:27-4:3 (“In the method, for each radio source, the first and second sets of data can include” access point information transmitted by the server to the mobile devices. “method may further comprise transmitting the third set of data from the service server to the user terminal...”)), Figs. 1-3.

136. *Vardi* discloses Limitation 1[pre].

ii. Limitation 1[a]:

1[a]	transmitting, by the server to a device, an authenticated access point list that includes at least one of a media access control (MAC) address or a service set identifier (SSID) of each of one or more authenticated access points, wherein the one or more authenticated access points are controlled by the server; and
------	---

137. In my opinion, *Vardi*, *IEEE802.11*, *Orava*, and *Yun* teaches this limitation.

138. In my opinion, after reviewing the '552 patent, the specification provides examples of what an “authenticated access point list” may contain but does not itself define the term.

139. I also understand that Petitioner’s contend for purposes of this Petition that the construction of an “authenticated access point list” is not outcome determinative. I agree.

140. FIG. 2 of the '552 patent “shows an illustrative example of an authenticated access point list and the corresponding specification provides that it may include the SSID or MAC address.

141. The Patent Owner (PO) in its infringement contentions raised that an “authenticated access point” is one that is saved from a previous connection and thus, an “authenticated access point lists” contains either the SSID or MAC address of access points that the mobile device previously connected to.

142. In my opinion, regardless of whether the authenticated access point list includes new or previously connected access point information, *Vardi* teaches it.

143. *Vardi* teaches a server sending an access point list information (API) that contains the information shown as illustrative in the ’552 patent. *See* Ex. 1007, 3:4-10.

144. *Vardi* explains that “clients receive updates about relevant access points from the server and use the information to select and connect to the preferred access point. The clients also check connectivity to other access points in the vicinity, and report the findings to the server. The server uses the reports to update its database, and sends corresponding updates to the clients.” *Id.*

145. *Vardi* lists the API shared from the server to the mobile devices, which includes both examples of API from the specification, the Network name (or SSID) and MAC address as shown below:

- i. Network name;
- ii. MAC address;

- iii. Received signal strength and variance over time;
- iv. Encryption status;
- v. Internet connection available capacity;
- vi. Access protocol response times;
- vii. Gateway IP address;
- viii. DNS address;
- ix. Occupied IP addresses;
- x. Captive portal credentials;
- xi. Connection Technology;

- xii. User Terminal Location;
 - xiii. Access Point Location;
 - xiv. Mapping Type—how an access point location was determined.
- The data base of data can comprise the above information as well as:
- i. Location
 - ii. Internet accessibility
 - iii. Long term behavioral statistics comprising:
 - Percentage of availability
 - Signal strength variance
 - Available bandwidth
 - iv. Name of owner;
 - v. Owner profile;
 - vi. Password.

146. A POSITA understands that “Network name” is synonymous with SSID. The meaning of SSID is “service set identifier”, which is simply the public text string that identifies a collection of access points that are configured as part of the same wireless network. Ex. 1007, 10:25-28 (“Network or AP name (SSID—service set identifier); and, AP Radio MAC address”).

147. *Vardi* teaches that the API transmitted from the server to the mobile device can include both previously connected APs as well as newly scanned APs. *See* Ex. 1007, 13:4-23.

148. Previously Connected APs. *Id.* (“If a ‘favorite’ AP (AP is called favorite if it is part of radio resource database that had been distributed to client...)”)

is detected by the IEEE 802.11 scan and the RSSI⁴ is above a predetermined threshold (ex. Owner's AP), the client can select this AP for connection or If a list of previously successfully used access points is available (locally stored) and some APs on the list are available... the client can select the AP... for connection.”)

149. Newly Discovered APs. *Vardi* explains when mobile devices operate in new areas, which is often the case with devices that remain on a person as they travel about their day, the mobile devices perform “IEEE scan” as *Vardi* refers to it, which a POSITA would recognize as an “Active Scan” as defined by IEEE 802.11, this scan produces a list of APs that are in the vicinity. *See* Ex. 1007, 12:30-39.

150. As *Vardi* explains, “when the mobile device is activated in a new location, it has no information in the cache to enable fast connection to an AP... when clients send connection reports they also send the cache information. Then, the server sends cache information to each client, relating to all APs in the vicinity of the client or in a geographical area requested by the client. In this manner, the mobile device can have cache information of APs to which the mobile device was not connected before.” *Id.*

⁴ *Vardi* goes beyond just searching for and connecting to a previous AP, it also performs an evaluation of the received signal strength (RSSI) and security evaluation “done by typical WiFi clients,” these additional steps are not required by the '552 patent, and thus, I omit them moving forward when citing the reference.

151. The only reference to “controlled by the server” in the specification (excluding the claims) was a single sentence at 4:33-35, which simply stated, “By way of example, but not limitation, the authenticated access point may include an access point controlled by mobile operating server 110 and/or an access point previously connected with end device 130.” (emphasis in original).

152. Figure 1 is the only figured that depicts both the mobile operating server and an access point.

153. Taking the two together, a POSITA would understand the plain and ordinary meaning of “controlled by the server” to mean or include a communication connection between the server and AP.

154. *Vardi* shows in FIG. 3, for example, that the server and AP are connected through the network. This, in my opinion, teaches “controlled by the server” as depicted by the ’552 patent’s FIG. 1.

155. I understand that claim 24 provides a further definition of “controlled by the server,” adding that “wherein to determine whether the at least one access point is the authenticated access point and is under control of the server, the determination unit determines whether the information regarding the at least one access point is included in the authenticated access point list.”

156. In my opinion, a POSITA would take claim 24 to mean that if an AP that was previously connected and, on the list, transmitted by the server to the mobile devices, the AP is “controlled by the server.”

157. *Vardi*, in my opinion, also teaches the definition provided by claim 24 that the AP was previously connected to by the mobile device and is included in the API transmitted by the server to the mobile device.

158. As *Vardi* explains, the server transmits access point information to the mobile devices and the mobile devices determines whether the AP from the scan is a preferred AP, an authenticated access point as it is referred to in the '552 patent, by comparing the scan results with the stored API.

159. If the stored API matches the scan, the mobile device determines that the AP is the preferred AP (authenticated access point) and connects. *See* Ex. 1007, 14:52-57 (“When client becomes active it executes an IEEE 802.11 scan for APs in reach and determines the SSID, MAC address... Using the MAC address, the client can compare this scan result with its radio resources database to determine which APs are preferred for connection and roaming.”)

160. *See also* Ex. 1007, 13:4-23 (“If a ‘favorite’ AP (AP is called favorite if it is part of radio resource database that had been distributed to client...) is detected by the IEEE 802.11 scan... (ex. Owner’s AP), the client can select this AP for connection or If a list of previously successfully used access points is available

(locally stored) and some APs on the list are available... the client can select the AP... for connection.”)

161. I have also considered the PO’s infringement contention theory that communication interaction (like I defined previously) satisfies this limitation; however, I understand that PO’s infringement contentions may narrow it to a specific communication interaction—namely, a probe request and response communication.

162. While I disagree with PO’s infringement contention that the mobile device is both the mobile device and the server, I have considered this theory as it applies to the references that I reviewed and, in my opinion, *Vardi* teaches this too.

163. *Vardi* explains that the mobile devices perform “IEEE 802.11 association procedure” beginning with “probing”, which a POSITA would readily understand means an IEEE 802.11 Active Scan. As I explained *supra*, Active Scan is a term of art that a POSITA would readily associate with issuing a probe request and waiting for a probe response. Here, *Vardi* teaches performing “probing to get association information.” Thus, a POSITA would readily have understood “probing to get association information” to encompass the client issuing a probe request and waiting for the AP to send a probe response.

164. *Vardi* continues to teach that “information acquired as part of the standard 802.11 scan, i.e., [Network or AP name (SSID—service set identifier); and,

AP Radio Mac address” is acquired by the mobile device performing the scan. Ex. 1007, 10:25-39.

165. In my opinion, *Vardi* teaches, or at least renders obvious, limitation 1[a].

166. Although *Vardi* teaches “IEEE scan,” “IEEE association procedure,” and “probing,” however, *Vardi* presumes knowledge and understanding of the IEEE 802.11 specification and thus, does not provide the underlying implementation details that a POSITA would know.

167. Because a POSITA would have a working knowledge of the IEEE 802.11 specification, or because *Vardi* explicitly directs a POSITA to review and consider the IEEE 802.11 specification, a POSITA would have found *Vardi*’s disclosure explicit.

168. Nonetheless, a POSITA would have naturally looked to *IEEE802.11* to ensure standard compliance and fill in any details regarding message formatting and thus, found it obvious to combine *Vardi* with *IEEE802.11*.

169. *IEEE802.11* defines what a mobile device must do during an “Active scan” procedure. The mobile device sends a probe request frame to various APs, and the receiving APs transmits a probe response frame to the mobile device as illustrated below:

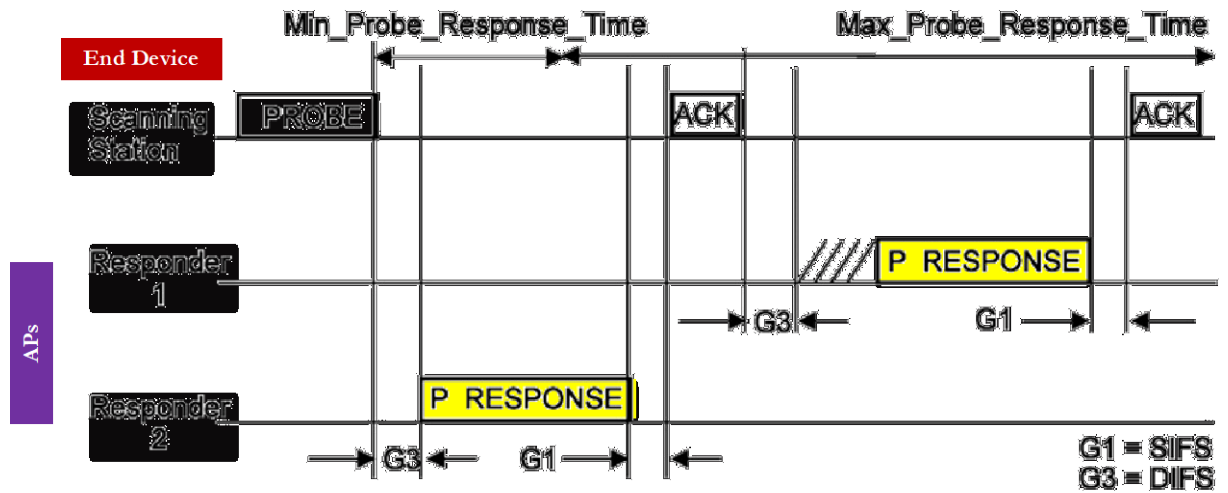


Figure 10-3—Probe response

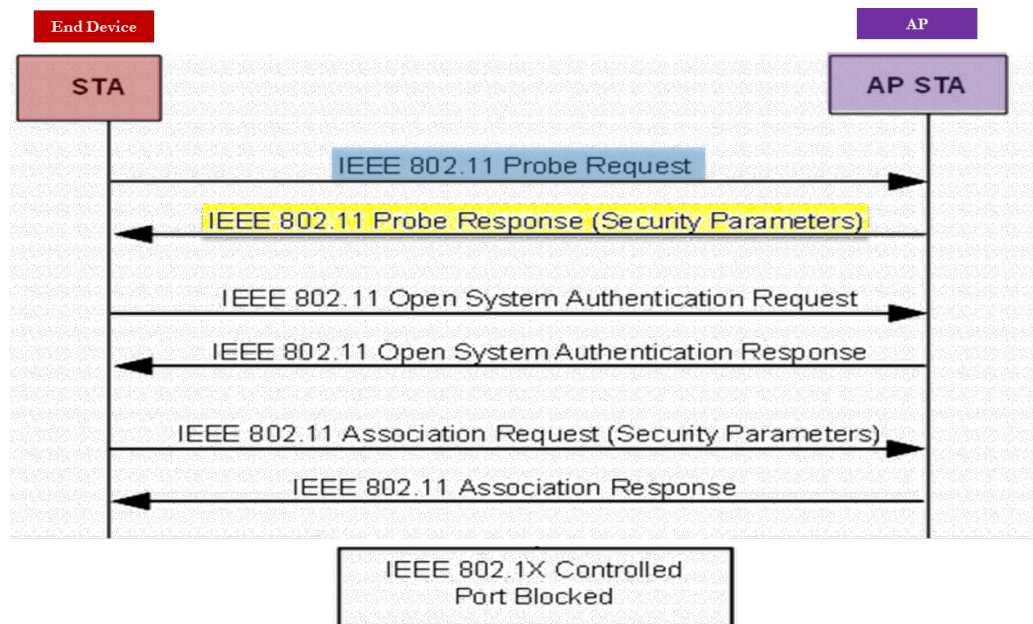


Figure 4-17—Establishing the IEEE 802.11 association

170. Figure 8-1 and Table 8-27 (portion) identifies the information contained within a probe response frame, including both the SSID and BSSID (MAC address) of the responding AP.

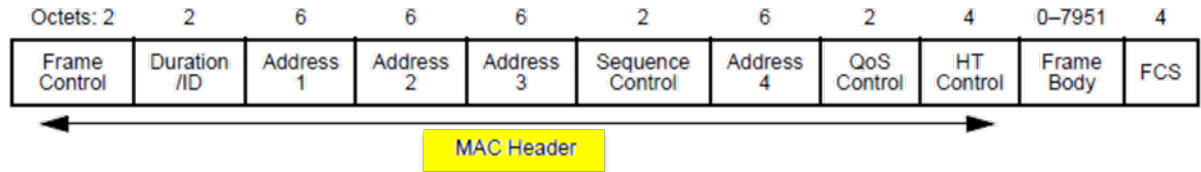


Figure 8-1—MAC frame format

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 8.4.2.2.
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set element is present within Probe Response frames generated by STAs using FH PHYs.

⋮

Order	Information	Notes
23	Measurement Pilot Transmission	The Measurement Pilot Transmission element is present if dot11RMMeasurementPilotActivated is between 2 and 7.
24	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RMMeasurementPilotActivated is between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 10.11.14) with two or more members, or if dot11MgmtOptionMultiBSSIDActivated is true, or if dot11InterworkingServiceActivated is true and the AP is a member of a Multiple BSSID Set with two or more members and at least one dot11GASAdvertisementID MIB attribute exists.

171. Although, in my opinion, *Vardi* teaches or at least renders obvious the access points are “controlled by the server,” *Orava* explicitly teaches a server assigning configuration parameters of the APs. Ex. 1005, ¶[54].

172. *Orava* explains that in “a server of the network, for example in the [] PAC, a list can be maintained to which the temporary MAC addresses allocated by the different access points AP are added. Thus, the AP can transmit a request for allocation of a temporary MAC address. On the basis of the request, the server selects an available address and transmits a response frame comprising the allocated address MAC.” *Id.*

173. This address assignment demonstrates that the server controls the AP.

174. As I explained above, a POSITA would have found it obvious to combine *Vardi*, *IEEE802.11*, and *Orava*. See Section IX.F.1.

175. In summary, but not limited to the following reasons, a POSITA would naturally look to *IEEE802.11* to provide the implementation details regarding “IEEE 802.11 scan” and “probing” because both *Vardi* and *Orava* explicitly direct a POSITA to the IEEE 802.11 standard and a POSITA would have a likelihood of success combining both *Vardi* and *Orava* because both explicitly direct a POSITA to use IEEE 802.11 standard.

176. Additionally, a POSITA would have found it obvious to combine *Orava*’s server management capabilities into *Vardi*’s server because *Vardi*, like *Orava*, discloses a multi-AP system “radio access points 370a-d,” enabling connections between mobile devices, APs, and the Internet.

177. A POSITA would have been motivated to and found it obvious to add *Orava*'s central server management capabilities, controlling the APs, to *Vardi*'s server because a POSITA would have understood the need to manage and distribute access point configurations within the system, for example, utilizing a single "SSID" for the "access points 370a-d."

178. It was well-known at the time of the alleged invention that APs within the same network broadcast the same SSID, for example, *Vardi*'s "'favorite' AP" and as a user moves floors in an office building, the device connects to different access points (all have unique MAC addresses) broadcasting the same SSID "'favorite' AP." Ex. 1007, 13:10-23.

179. Additionally, *Orava*'s assures that the randomly generated Fake IDs will be unique across APs by allocating specific MAC address space per AP. Ex. 1005, ¶[54] ("In a server of the network... a list can be maintained to which temporary MAC address allocated by the different [] AP are added... the server selects an available address and transmits a response...").

iii. Limitation 1[b]

1[b]	transmitting, by the server to the device, a fake device identifier, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to
------	---

falsely identify the device in a probe request frame in a search
for at least one of the one or more authenticated access points
around the device.

180. In my opinion, *Vardi*, *IEEE802.11*, *Orava*, and *Yun* teaches this limitation.

181. *Vardi* teaches IEEE 802.11-standard compliant probing, which transmits a MAC address in the probe request frame to the AP and, in response, the AP transmits a probe response comprises its SSID, MAC address, and numerous other fields defined in IEEE 802.11. But *Vardi* does not teach generating “a fake device identifier” for use in the probe request frame. *Orava* does.

182. *Orava* explains that mobile device generates a REF identifier that it transmits to a central server (referred to as PAC) where the central server or PAC generates a random fake device identifier and then, in response to the mobile device’s message, transmits the fake device identifier for use by the mobile device for “all protocol messages.” Ex. 1005, ¶¶[26], [32], [34], and [49].

183. *Orava* explains two embodiments for the server generating the fake device identifier both teach this limitation, and both are compatible with each other. Ex. 1005, ¶[26].

184. *Orava* teaches that “MT transmits a request comprising the identifier it has determined to a second device to arrange a temporary MAC address. The second device may be a second terminal MT, an access point AP or a public access controller PAC, depending on the configuration of the system... On the basis of the request, a temporary MAC address MAC can be arranged in the second device to be used... The second device transmits a response frame relating to the arrangement of the MAC address comprising an identifier (MAC/REF). The MT identifies on the basis of the identifier that the response frame is intended for it. On the basis of the response frame, if the MAC address has been successfully allocated, the terminal MT can start using the MAC address allocated to it...,” the first option.

185. Additionally, *Orava* explains, that “the second device allocates a temporary MAC address MAC on the basis of the request... the identifier mentioned in step 202 is a particular reference identifier REF, which is only used to request 203 for allocation of a MAC address and to respond to it in order for the MT being able to recognize that the response frame is intended for it,” the second option.

186. Both teach a mobile device receiving from a server a fake device identifier.

187. *Orava* explains that the “control of temporary MAC addresses may be centralized for instance in a public access controller PAC.” Ex. 1005, ¶[32].

188. *Orava*'s fake device identifier (Fake ID) can be generated utilizing one of a number of methods. *Orava* describes the Fake ID "MAC can be a random number generated by means of a random number generator. MAC can be selected from the address space allocated to the MT on the basis of an address selection algorithm. A temporary MAC address MAC can be allocated to the MT for instance from among organization-specific unique identifiers (OUI) reserved for this purpose. Typically, one OUI allows 2^{24} addresses. The IEEE 802 MAC address format allows locally administrable MAC addresses, in which there are 46 available bits in a 48-bit address format for selecting the temporary MAC address. A MAC address can also be formed of a network identifier, such as a BSS identifier BSSID, and of a random part added thereto, for example." Ex. 1005, ¶[30].

189. Each of *Orava*'s generation algorithms results in a Fake ID that includes either a random character or number as required by the claim; however, *Orava* details that its Fake ID is generated in "IEEE 802 MAC address format ... in which there are 46 available bits in a 48-bit address format for selecting the temporary MAC address." Id.

190. In my opinion, it would have been obvious to a POSITA to apply the randomly generated MAC address to *Vardi*'s probing message as defined by *IEEE802.11*.

191. As I explain in more detail in Section X, a POSITA would have a high likelihood of success adding *Orava*'s random generation capabilities to *Vardi*'s server.

192. *Orava* explicitly informs a POSITA that "MAC" follows the IEEE MAC address format, *IEEE802.11* "allows locally administrable MAC addresses." Ex. 1005, ¶[30].

193. *Orava* teaches that "[p]referably, the use of a temporary MAC address MAC does not, after arrangement of the address, differ in any way from the use of a fixed MAC address permanently allocated by the manufacturer. The temporary MAC address can thus be used instead of a fixed address in all protocol messages." Ex. 1005, ¶[49].

194. As detailed above, in my opinion, *Vardi* discloses transmitting a probe request frame. It was well-known at the time of the alleged invention that the probe request frame included the "real" MAC address. See Ex. 1001, 3:4-18 (describing the alleged problem with IEEE 802.11 "the end device may transmit a probe request frame that may include a device identifier, for the end device such as a media access control (MAC) address of the end device").

195. *Orava* informed a POSITA that "the fixed MAC address determined by manufacturers cause a security risk: a MAC address can be picked up from every message transferred over the air interface..." Ex. 1005, ¶[3].

196. Thus, a POSITA would have found it obvious to swap *Vardi*'s "real" MAC address for *Orava*'s randomly generated Fake ID. Particularly because *Orava*'s Fake ID is in IEEE 802 MAC format, *Orava* instructs a POSITA that use of the Fake ID should not "differ in any way from the use of a fixed MAC address," and that the Fake ID can be used in "all protocol messages." Ex. 1005, ¶¶[30], [49].

197. As explained above, "real" MAC address are themselves randomly generated and thus, a POSITA would have a high likelihood of success swapping one randomly generated number for another. Particularly true here, where *Orava* generates the Fake ID to remain IEEE 802.11 compliant.

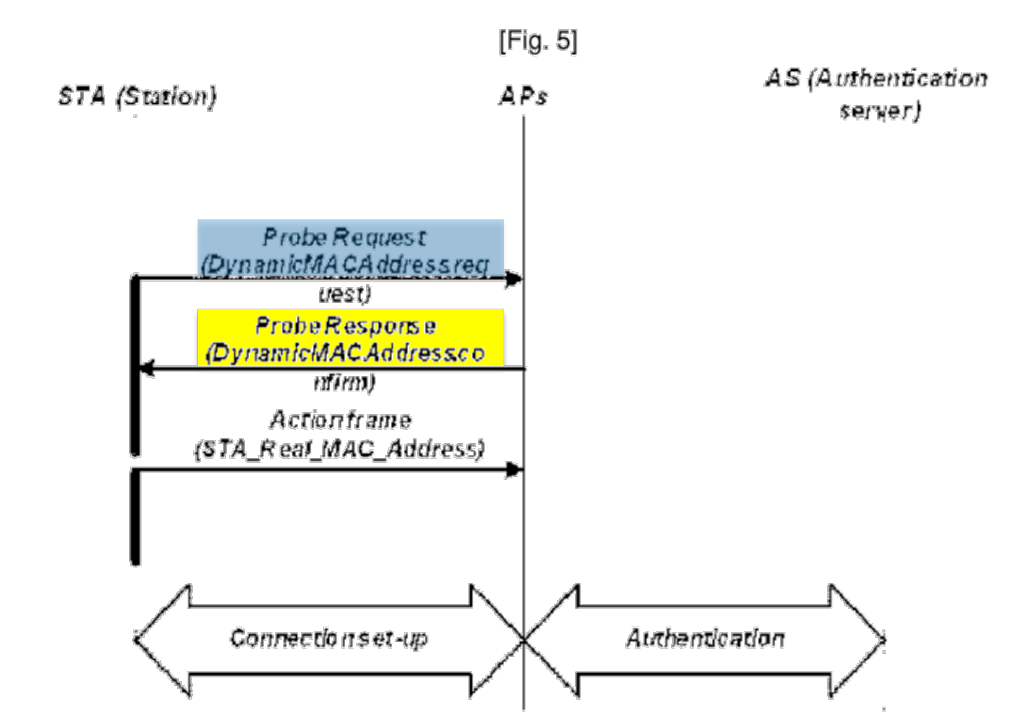
198. The combination requires a simply plug-n-play between the "real" MAC address and the Fake ID randomly generated.

199. In my opinion, the *Vardi-Orava* system is explicit, *Orava* informs a POSITA that the Fake ID can be used in "all protocol messages" and thus, a POSITA would readily have understood that "all protocol messages" includes a probe request frame. *Yun* confirms my opinion.

200. In considering whether any additional prior art discloses transmitting a Fake ID in the probe request, to the extent that PO contends *Vardi-Orava*'s teachings are not explicit. *Yun* is explicit. *Yun*, Fig. 5, ¶¶[154]-[156].

201. Yun explains that “the transmitted packet on air uses an arbitrary MAC address (‘Dynamic MAC address’) which is dynamically allocated.” Ex. 1004, ¶[154].

202. Yun further explains “the station(12) transmits the data including the MAC address request such as the probe request(‘Dynamic MAC address request’) to the access points(14).” Ex. 1004, ¶[156].



203. Yun explicitly directs a POSITA to using the received generated Fake ID in a “probe request” to have “MAC address anonymity[, which] makes an identity of the station(12) not presumed through the MAC address.”

204. A POSITA would have found it obvious to combine *Vardi*, *Orava*, and *Yun* to transmits the received MAC address (*Orava*) in the probe request frame (*Vardi/IEEE802.11*). See Section IX.F.1.

205. As I explain above, *Vardi*, *Orava*, and *Yun* utilize *IEEE802.11* probe request/response frame exchanges to communicate with APs.

206. *Orava*'s Fake ID is formatted as an IEEE802 MAC address and, thus, only requires exchanging one set of characters for another set explaining that the Fake ID can be used the same as the fixed MAC address in "all protocol messages." Ex. 1005, ¶[49].

207. And *Yun* explicitly discloses transmitting the Fake ID in the probe request frame. See *id.*, FIG.5, ¶¶[154-156].

208. Again, a POSITA would have a high likelihood of success combining *Vardi*, *IEEE802.11*, *Orava*, and *Yun* to plug-n-play the Fake ID (randomly generated in IEEE 802.11 MAC format) for the "real" MAC address (randomly generated) into the 802.11 standard probe request frame. Such a substitute was conventional and well-known at the time of the alleged invention. See Section IX.F.1.

2. Claim 2

Claim 2	The method of claim 1, wherein the one or more authenticated access points include a Wi-Fi access point.
---------	--

209. In my opinion, *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 2.

210. *Vardi* teaches that the APs provide Wi-Fi (e.g., wireless Internet access). Ex. 1007, 14:66-15:1 (“In FIG. 3, a computing resource, such as server 310, and radio access points 370 a-d are connected to a network 305, such as the Internet. In this embodiment, access point 370 d belongs to a user who also uses access device 320, such as a laptop, a PDA, etc. The user generally is able to access the Internet 305 by connecting device 320 to access point 370 d wirelessly.”)

211. Additionally, *Vardi* explains that the mobile devices communicate with the APs via Wi-Fi standards and enabled components. Ex. 1007, 9:54-59 (“clients continuously collect radio resources information about APs detected by the wireless user terminal. These clients can be executed on laptops, handheld devices (PDA[s]), cellphones, or any other devices that incorporates a radio facility for wireless communication, such as WiFi.”); 5:11-16 (“Wifi enabled mobile telephones”).

212. Further, FIG. 3 of *Vardi* illustrates a mobile device in wireless communication with APs connected to the Internet 305. *See also* Ex. 1005, FIG. 1, ¶[19] (“shows a telecommunications system ... The system comprises a terminal device MT and a WLAN network WAN according to any version of the *IEEE802.11* standard.”).

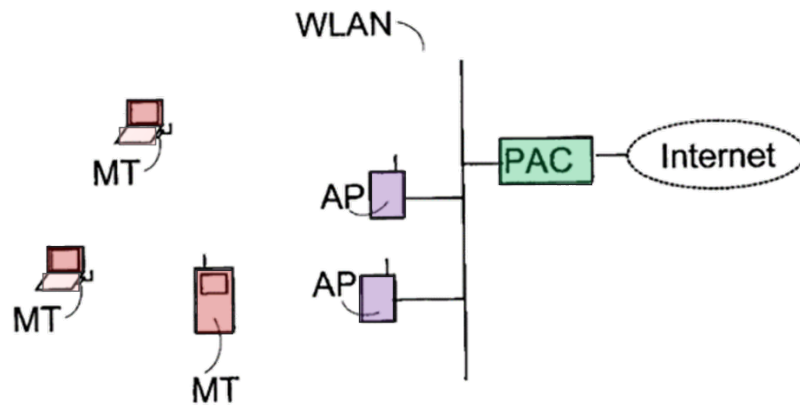


Fig. 1

3. Claim 3

Claim 3	The method of claim 1, wherein the transmitting the fake device identifier includes transmitting a fake media access control (MAC) address.
---------	---

213. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 3.

214. In my opinion, *Vardi* teaches transmitting the MAC address to the AP during “probing”; however, *Vardi* does not teach transmitting a fake device identifier in its place.

215. But as I explained above in limitation 1[b], *Orava* teaches that the fake identifier is in “IEEE 802 MAC address format...in which there are 46 available bits in a 48-bit address format for selecting the temporary MAC address.” See limitation 1[b]; Ex. 1005, ¶¶[30][49].

216. Additionally, *Yun* explicitly teaches transmitting the Fake ID in a probe request frame. *Yun*, ¶[145].

4. Independent Claim 4

217. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious Claim 4.

i. Limitation 4[pre]:

4[pre]	A method performed by an access point, the method comprising:
--------	---

218. I understand that the preamble of claim 4 merely states the purpose or intended use of the claimed subject matter, which is not limiting.

219. In my opinion, *Vardi* teaches the preamble.

220. *Vardi* teaches a wireless communication system including a server, a mobile device, and an access point. *Vardi* explains that the “invention relates to accessing wireless services and locating and mapping wireless access points that provide access to wireless services,” the claimed “method performed by an access point.” *Vardi* at 1:19-21.

ii. Limitation 4[a]:

4[a]	receiving, by the access point from a device, a probe request frame that includes a fake device identifier for the device, wherein the fake device identifier is received at the device from a server, and wherein the fake device identifier includes at least
------	---

one of one or more random numbers or one or more random characters;

221. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious this limitation.

222. *Vardi* discloses that the AP receives “probing” messages from the mobile devices, which includes the “real” MAC address. *Vardi* discloses, “[c]onnecting to a wireless network starts by scanning the neighborhood for candidate AP connections (IEEE 802.11 scan). The IEEE 802.11 scan can produce a list of access points in reach.” Ex. 1007, 13:4-7.

223. A POSITA would have readily understood that an “IEEE 802.11 scan” corresponds to the IEEE 802.11 Active scan procedure. An IEEE 802.11 scan is a well-understood term of art encompassing frame exchange sequence for “probe request/response , authentication, association.” to locate nearby APs. Applicants’ admitted prior art confirms this. Ex. 1001, 3:4-18 (“to connect to a [] (WLAN), an **end device may search for at least one available access point** around the end device... When searching, the end device **may transmit a probe request frame that may include a device identifier, for the end device such as a [] (MAC) address of the end device**... since the **probe request frame that includes the device identifier is transmitted to access points** around the end device, present location information of the end device may be exposed...”).

224. That is, a POSITA reading *Vardi* would understand that its IEEE scan begins with the client transmitting a probe request frame and the APs within reach receiving the probe request frame and, in response, transmitting a probe response frame to the client “produc[ing] a list of access points in reach,” as shown below. Ex. 1007, 13:4-7.

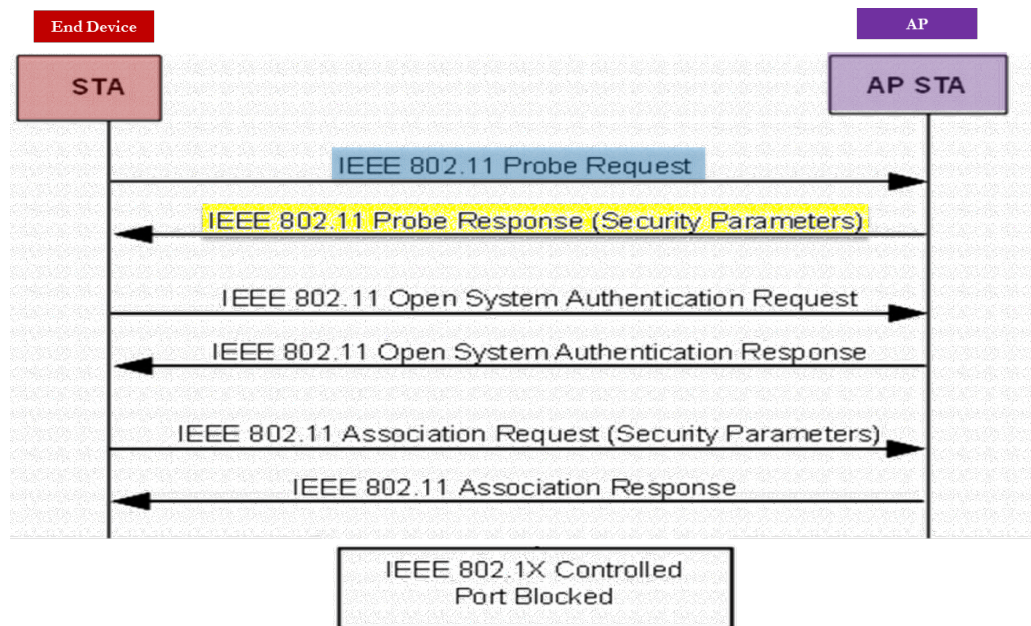


Figure 4-17—Establishing the IEEE 802.11 association

225. *Vardi*, however, does not disclose using a “fake identifier,” where the “fake identifier” includes either a random number or character.

226. First, it is well-known that MAC addresses themselves are randomly generated per manufacturer. Ex. 1005, ¶[3] (“for WLAN networks according to *IEEE802.11* specifications, IEEE allocates an OUI identifier (Organizationally

Unique Identifier) to each manufacturer, on the basis of which identifier the manufacturer can determine MAC addresses for the devices.”).

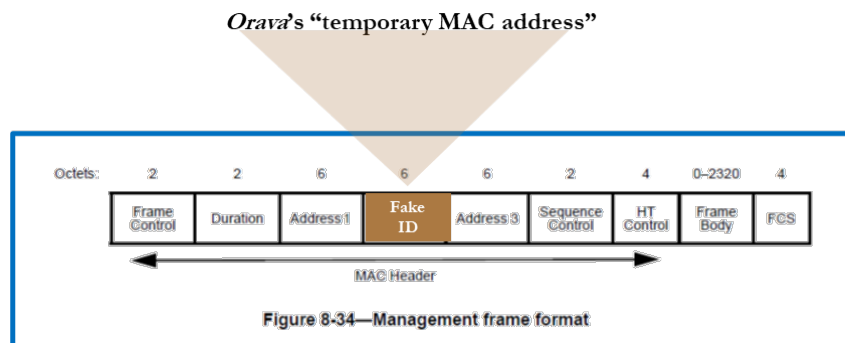
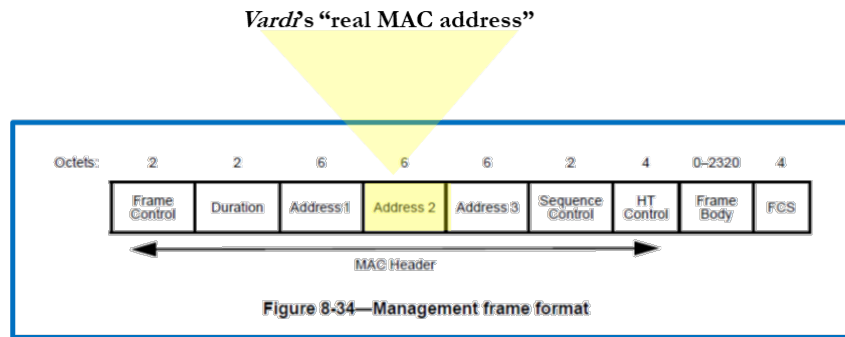
227. So, the use of random generated MAC addresses within a probe request frame is the normal operation.

228. Second, as explained above, the use of random generated MAC addresses or Fake ID, different from the “real,” within IEEE 802.11 protocol messages was also well-known. *See e.g.*, Ex. 1005, ¶[49]; *Yun* ¶[156].

229. *Yun*, explicitly discloses the “***transmitted packet on air uses an arbitrary MAC address*** (‘Dynamic MAC address’)” to provide “MAC address anonymity.” Ex. 1004, ¶[154].

230. *Yun* further teaches that the “station(12) transmits the data including the MAC address request such as the probe request(‘Dynamic MAC address request’) to the access points(14).” Ex. 1004, ¶[156]

231. It was also obvious to a POSITA to substitute *Vardi*’s real MAC address with *Orava*’s received Fake ID in *Vardi*’s probe request frame (as illustrated below).



232. Additionally, *Vardi*, *Orava*, and *Yun* presume knowledge of the underlying standard and thus, they do not provide the implementation details.

233. However, a POSITA would understand the workings of “probing,” and transmitting a frame within a “probe message.” Regardless of whether the POSITA possessed that working knowledge, *Vardi*, *Orava*, and *Yun* direct a POSITA to look to *IEEE802.11* for those details.

234. *IEEE802.11* defines the implementation details underpinning *Vardi*, *Orava*, and *Yun*. As identified below, the *IEEE802.11* probe request frame includes transmitting a MAC address—(e.g., Address 2)—within the probe request sent by the device to the AP. *IEEE802.11*, FIGS. 4-17, 8-34; 10-3.

10.1.4.3.3 Active scanning procedure

Upon receipt of the MLME-SCAN.request primitive with ScanType indicating an active scan, a STA shall use the following procedure:

For each channel to be scanned:

- Wait until the ProbeDelay time has expired or a PHYRxStart.indication primitive has been received.
- Perform the Basic Access procedure as defined in 9.3.4.2.
- Send a probe request to the broadcast destination address, with the SSID and BSSID from the MLME-SCAN.request primitive. When the SSID List is present in the MLME-SCAN.request primitive, send one or more probe request frames, each with an SSID indicated in the SSID List and the BSSID from the MLME-SCAN.request primitive.
- Set to 0 and start a ProbeTimer.
- If PHY-CCA.indication (busy) primitive has not been detected before the ProbeTimer reaches MinChannelTime, then set NAV to 0 and scan the next channel, else when ProbeTimer reaches MaxChannelTime, process all received probe responses.
- Set NAV to 0 and scan the next channel.

See Figure 10-3.

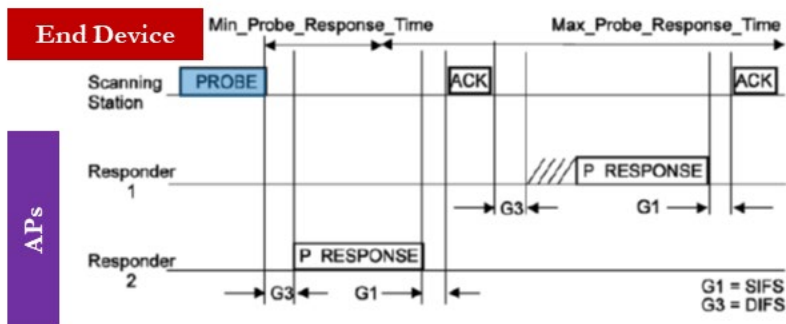


Figure 10-3—Probe response

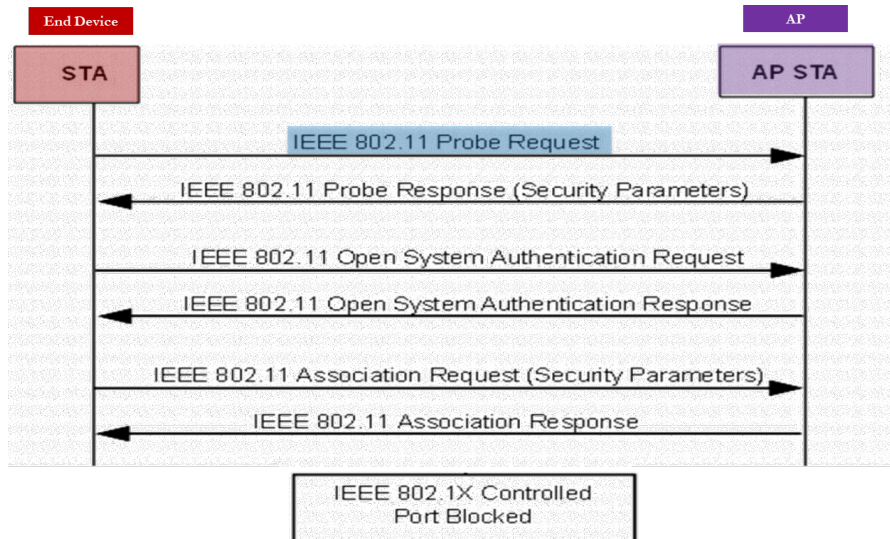
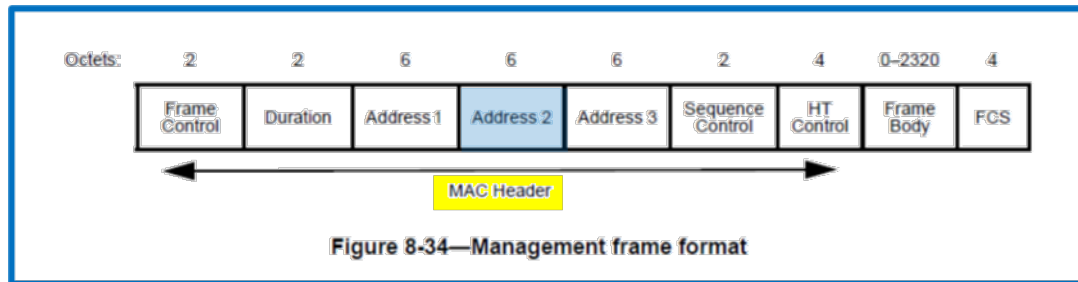


Figure 4-17—Establishing the IEEE 802.11 association



The address fields for all management frames except Multihop Action frames are as follows:

- a) The Address 1 field of the management frame is the RA (=DA) and is determined as the destination of the frame.
- b) The Address 2 field of the management frame is the TA (=SA) and is determined as the address of the STA transmitting the frame.
- c) The Address 3 field of the management frame is set and determined as follows:
 - 1) In management frames of subtype Probe Request, the Address 3 field is the BSSID. The BSSID is either a specific BSSID as described in item 4) below or the wildcard BSSID as defined in the procedures specified in 10.1.4.
 - 2) In management frames of subtype Action, Category Public, the Address 3 field is the BSSID. The BSSID value is set according to 10.19.
 - 3) If dot11OCBAActivated is true, the Address 3 field is the wildcard BSSID.
 - 4) Otherwise:
 - i) If the STA is contained within an AP or is associated with an AP, the Address 3 field is the BSSID. The BSSID is the address currently in use by the STA contained in the AP.
 - ii) If the STA is contained within an AP or is transmitting the management frame to an AP, the Address 3 field is the BSSID. The BSSID is the address currently in use by the STA contained in the AP.
 - iii) If the STA is transmitting the management frame to one or more members of an IBSS, the Address 3 field is the BSSID of the IBSS.
 - iv) If the STA is a mesh STA, the Address 3 field is the TA.

235. It would have been obvious to a POSITA at the time of the alleged invention to transmit *Orava*'s received Fake ID as part of *Vardi*'s probing message from the mobile device to the AP as *Orava* explains that the Fake ID can be used the same as the fixed MAC address in "all protocol messages." *Yun* confirms this position. Ex. 1004, ¶¶[154-156]; see also Section IX.F.1.

236. *Orava* informed a POSITA that "fixed MAC address determined by manufacturers cause a security risk: a MAC address can be picked up from every message over the air interface..." ¶[3].

237. *Orava* explains, “[i]n order to arrange anonymity, it has been suggested that temporary MAC addresses be used for WLAN networks.” ¶¶[4], [27] (“FIG. 2 allows temporary MAC addresses to be arranged reliably and the user to be provided with anonymity...”).

238. *Yun* likewise informed a POSITA that it wants to “protect a MAC address” and “MAC address anonymity makes an identity of the station(12) not presumed through the MAC address.” Ex. 1004, ¶[154].

239. *Yun*’s disclosure further emphasizes that a POSITA would have found it obvious and been successful transmitting a probe request including a Fake ID.

240. And each reference—*Vardi*, *Orava*, and *Yun*—explicitly disclose devices implementing IEEE 802.11 compliant MAC addresses. *See* Section IX.F.1

241. Also, in view of *Orava*’s and *Yun*’s teachings of the security risk, would know that continuing to use the real MAC address exposed the user to location tracking and privacy concerns. Ex. 1005, ¶¶[3], [29-30]; Ex. 1004, ¶¶[154]-[156]; *see also* Section IX.F.1.

iii. Limitation 4[b]:

4[b]	transmitting, by the access point to the device, a probe response frame that includes information regarding the access point;
------	---

242. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious this limitation.

243. As explained in 4[a], a POSITA reading *Vardi* would understand that its “IEEE 802.11 scan” and “IEEE 802.11 association procedure” encompasses the client transmitting a probe request frame, the APs within reach receiving the probe request frame, and transmitting a probe response frame to the client as shown below.

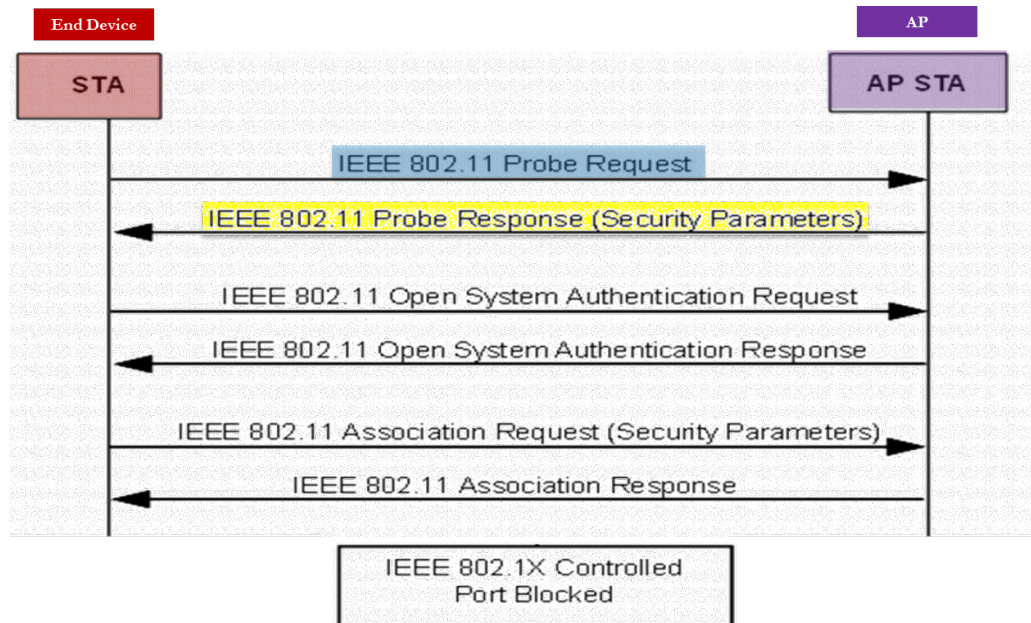


Figure 4-17—Establishing the IEEE 802.11 association

244. *Vardi* explains that the “IEEE 802.11 scan can produce a list of access points in reach.” A POSITA would understand that the list is produced by the mobile device receiving probe responses as shown below. Ex. 1007, 13:4-7.

245. While *Vardi* does not expressly use the words “probe response frame,” it does explain that the mobile device receives a list of access points in reach from

“probing,” and the information received from the scan includes the information as defined by the 802.11 standard. Ex. 1007, 13:4-7, 10:25-36.

246. That is, the mobile devices perform a “Basis IEEE 802.11 association procedure... using... probing to get association information” and the AP, in response, provides “information [] as part of the standard 802.11 scan, i.e.: Network or AP name (SSID—service set identifier); and, AP Radio MAC address” to the mobile device.” Ex. 1007, 10:25-36.

247. *Vardi* also teaches “When [the] client becomes active it executes an IEEE 802.11 scan for APs in reach and **determines the SSID, MAC address...**” A POSITA would have known that the SSID and MAC address are defined items included in the probe response frame. Ex. 1007, 14:52-57.

248. Thus, in my opinion, *Vardi* teaches or at least renders obvious limitation 4[b].

249. However, to the extent *Vardi*’s disclosures are not explicit enough, a POSITA would have naturally looked to *IEEE802.11* to fill in ally alleged gaps or simply because *Vardi* directs a POSITA to an “IEEE scan” or “IEEE association.”

250. *IEEE802.11* defines the communication and frame for a probe request and probe response exchange. Here, as shown below, *IEEE802.11* provides the MAC Header (reproduced below) and the definition of a “Probe Response frame body” in Table 8-27 (a portion of which is also reproduced below).

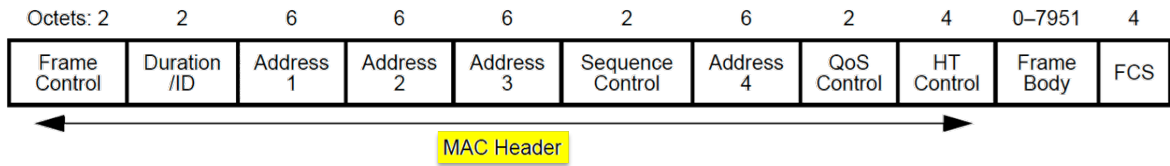


Figure 8-1—MAC frame format

Table 8-1—Valid type and subtype combinations

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110	Timing Advertisement

Table 8-1—Valid type and subtype combinations (continued)

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication

251. Table 8-27—Probe Response frame body is a management frame and is transmitted with a MAC header. The MAC Header and Table 8-27 outlines “information regarding the access point” that is transmitted by the AP to the mobile device as part of the “probe response” frame.

iv. Limitation 4[c]

4[c] receiving, by the access point from the device in response to the transmitting the probe response frame, a connection request that includes an authentic device identifier for the device, wherein the receiving the connection request⁵ includes receiving the connection request in response to an authentication of the access point based on an authenticated point list received at the device from the server, and wherein the authenticated point list includes information that indicates that the access point is an authenticated access point; and

252. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious this limitation.

253. *Vardi* teaches mobile devices establishing a connection to its preferred AP, for example, “‘favorite’ AP” to gain access to the Internet by performing “IEEE 802.11 association procedure” and comparing the scan results with the access point

⁵ I have been asked to consider “connection request” under PO’s infringement theory for purposes of this proceeding. I reserve the right to point to different disclosures for a “connection request” if PO changes their definition or the Board issues a construction for the term.

information received from the server to determine that the AP is the preferred AP.
Ex. 1007, 13:13-17.

254. *Vardi* teaches or at least renders obvious transmitting a connection request to the preferred AP comprising an authentic device identifier, for example, the MAC address.

255. *Vardi* describes “[i]f a ‘favorite’ AP (AP is called favorite if it is part of radio resource database that had been distributed to client)... is detected by the IEEE 802.11 scan... the client can select this AP for connection...”

256. IEEE 802.11 is a term of art, which a POSITA would have readily understood corresponds to the “Active Scan” process, which includes the mobile device transmitting a probe request and the AP transmitting, in response, a probe response.

257. Here, *Vardi*’s mobile device transmitted a probe request and “‘favorite’ AP” transmitted, in response, a probe response frame to the mobile device. *Vardi*’s mobile device compared its “radio resource database that had been distributed to [it]” from the server with the probe response and compared the “MAC address” to determine that “‘favorite’ AP” is its preferred AP and established connection.

258. *Vardi*, like the asserted patents, presume a working knowledge of *IEEE802.11* and thus, do not provide the underlying implementation details a POSITA would readily understand at the time of the invention.

259. However, *Vardi* provides numerous disclosures to support that a POSITA would have found *Vardi* teaches or at least renders obvious issuing a connection request including the authentic device identifier.

260. *Vardi* explains that “[w]hen client becomes active it **executes an IEEE 802.11 scan** for APs in reach and determines the SSID, MAC address... Using the MAC address, the client can compare the scan result with the radio resource database to determine which **APs are preferred for connection** and roaming.” *Id.*, 14:52-57.

261. *Vardi* explains that **“[c]onnecting to a wireless network starts by scanning** the neighborhood for candidate **AP connections** (IEEE 802.11 scan). The IEEE 802.11 scan can produce a list of access points in reach.” Ex. 1007, 13:4-7.

262. Further, *Vardi* teaches that the **mobile device** performs a “Basis **IEEE 802.11 association procedure (inclusive of WEP, if needed)**; either using beacon information or ***probing to get association information***” and the results of that scan comprise “Network or AP Name (SSID service set identifier); and, AP Radio MAC address.” Ex. 1007, 10:26-36.

263. *Vardi* also explains that “establishing a WiFi connection to the Internet requires a sequence of steps, starting with the IEEE 802.11 association...” Ex. 1007, 7:36-40.

264. A POSITA would have found each of these disclosures illustrative of a mobile device issuing a connection request as defined by *IEEE802.11*. Particularly, *Vardi*'s disclosure of a mobile device performing “**Basic IEEE 802.11 association procedure (inclusive of WEP, if needed)**” and “**establishing a WiFi connection to the Internet**” requires a **sequence of steps**, starting with the **IEEE 802.11 association...**”

265. Because *Vardi* refers to IEEE 802.11 association procedure as “**a sequence of steps**” to “establish a WiFi **connection** to the Internet” a POSITA at the time of the alleged invention would have readily understood *Vardi* as teaching the mobile device and AP proceed through each of the three steps until a connection to the Internet is established.

266. That is, *Vardi* teaches “probing” (exchanging probe request/response frames), using “WEP” (authentication frames), and establishing WiFi connection to the Internet (association request/response frames).

267. Moreover, a POSITA knows that *Vardi*'s “IEEE 802.11 procedure must include three major steps as defined in *IEEE802.11*: (1) device discovery (“probing”); (2) device authentication (WEP, checking capabilities); and (3) establishing connection (association)” for the mobile device to “establish[] a connection to the Internet.”

268. Therefore, a POSITA would have readily understood at the time of the alleged invention that *Vardi* teaches or suggest a “connection request” and because *Vardi*’s disclosure is an “IEEE 802.11 association procedure,” a POSITA would have understood that the transmitted messages are defined by the standard and thus, the authentication and association frames include a MAC header, which comprises the MAC address of the mobile device.

269. The contents of a probe request/response, authentication request/response, and association request/response frame were well-known at the time of the alleged invention. The asserted patents themselves acknowledge this. Ex1001, 3:4-18 (describing the problem with IEEE use of MAC addresses “in order to connect to a wireless local area network (WLAN), an end device may search for at least one available access point around the end device. By way of example, but not limitation, the access point may be a Wi-Fi access point and the WLAN may be a Wi-Fi network. When searching, the **end device may transmit a probe request frame that may include a device identifier, for the end device such as a media access control (MAC) address of the end device.** In such cases, **since the probe request frame that includes the device identifier is transmitted to access points around the end device,** present location information of the end device may be exposed to some access points with which a user of the end device does not want to

be connected and/or other devices to which the end device does not want to disclose the present location information.”). *See IEEE802.11*.

270. Because *Vardi* presumes knowledge of IEEE 802.11 and explicitly directs a POSITA to its teachings, it is also my opinion, that a POSITA would have found it obvious to combine the underlying implementations details provided by *IEEE802.11* to *Vardi*’s communication system.

271. Particularly, *Vardi* directs a POSITA that the mobile device’s client performs IEEE authentication and association, that would naturally guide a POSITA to review the details of an IEEE authentication and association procedure to ensure compliance with the specification.

272. *IEEE802.11* defines that a “STA shall be able properly to construct a subset of the frames specified in this clause for transmission and to decode... All STAs shall be able to validate every received frame... and to interpret certain fields from the MAC headers of all frames.” *IEEE802.11*, 380.

273. It continues that “[e]ach frame consists of the following... *MAC header*... A variable-length *frame body*, which contains information specific to the frame *type* and *subtype*...” *IEEE802.11*, 380 (emphasis in original).

274. The general frame format transmitted includes a MAC Header followed by the frame body, which is depicted in Figures 8-1 and 8-2 (shown below).

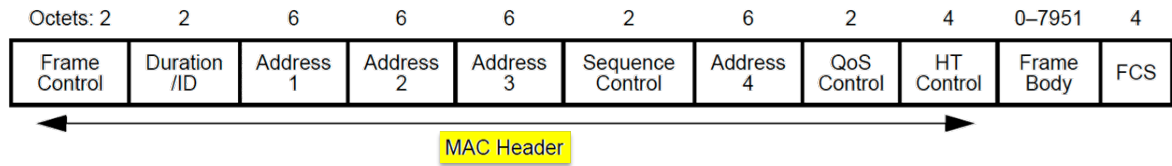


Figure 8-1—MAC frame format

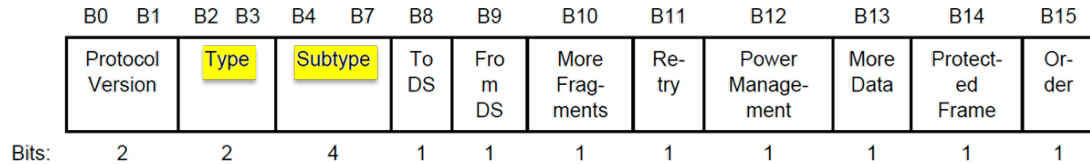


Figure 8-2—Frame Control field

275. Table 8-1 identifies valid type and subtype combinations. This is important because it identifies to a POSITA that “Association request,” “Association response,” “Authentication request,” and “Authentication response” are each of type “Management,” which dictates that it is transmitted with the MAC Header.

Table 8-1—Valid type and subtype combinations

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110	Timing Advertisement

Table 8-1—Valid type and subtype combinations (continued)

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication

276. Additionally, Figure 4-17 of *IEEE802.11* (shown below) corresponds to the same evidence cited to by PO in its infringement contention theory I was asked to consider.

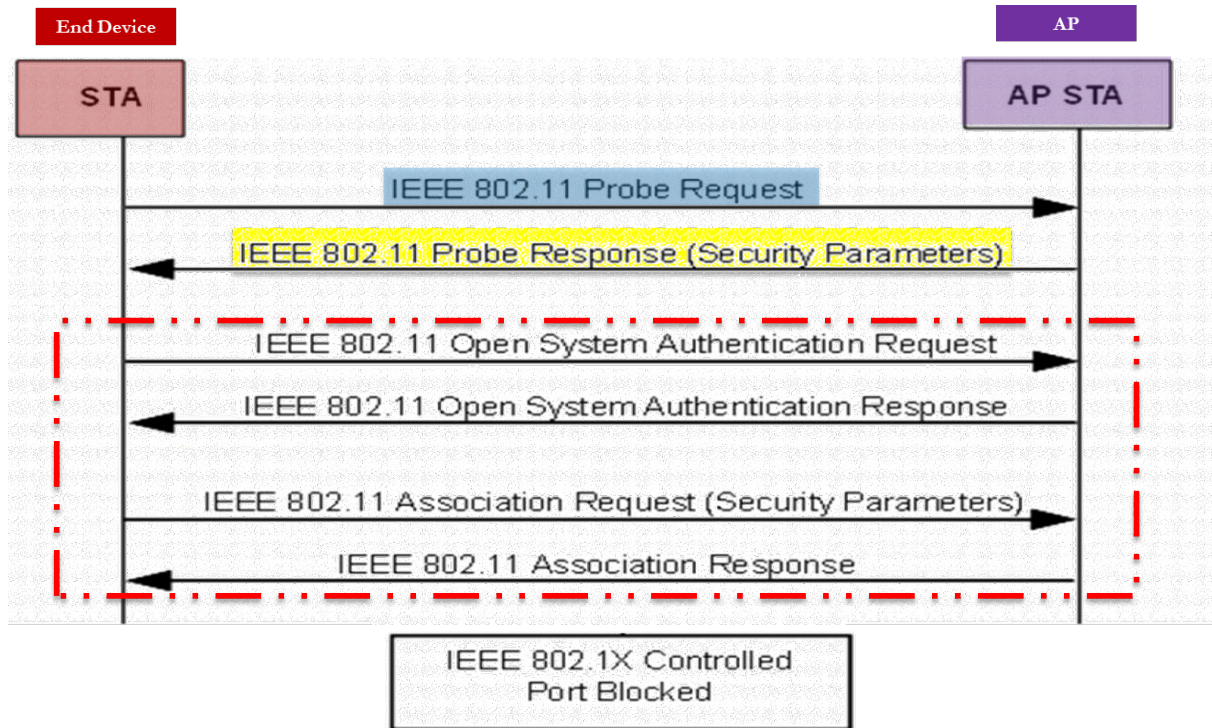


Figure 4-17—Establishing the IEEE 802.11 association

277. The combination of this evidence supports my opinion that a POSITA would have found it obvious to combine *Vardi* with *IEEE802.11* to render obvious this limitation.

5. Claim 5

278. *Vardi* in view of *IEEE802.11* and *Orava* render this claim obvious.

- i. Limitation 5[a]:
- ii. Limitation 5[b]:
- iii. Limitation 5[c]:

-
- 5 [a] The method of claim 4, further comprising: receiving, from the device, an association request;
-
- 5 [b] transmitting, to the device, an association response to the association request; and
-
- 5 [c] facilitating connection of the device to a communication network via the access point in accordance with the association response.
-

279. *Vardi, IEEE802.11, Orava, and Yun* render obvious claim 5.

280. In my opinion, claim 5 merely recites the steps outlined by *IEEE802.11* for connecting a mobile device to the Internet. For example, Figure 4-17 from *IEEE802.11* illustrates this procedure for an “Open System” authentication and association.

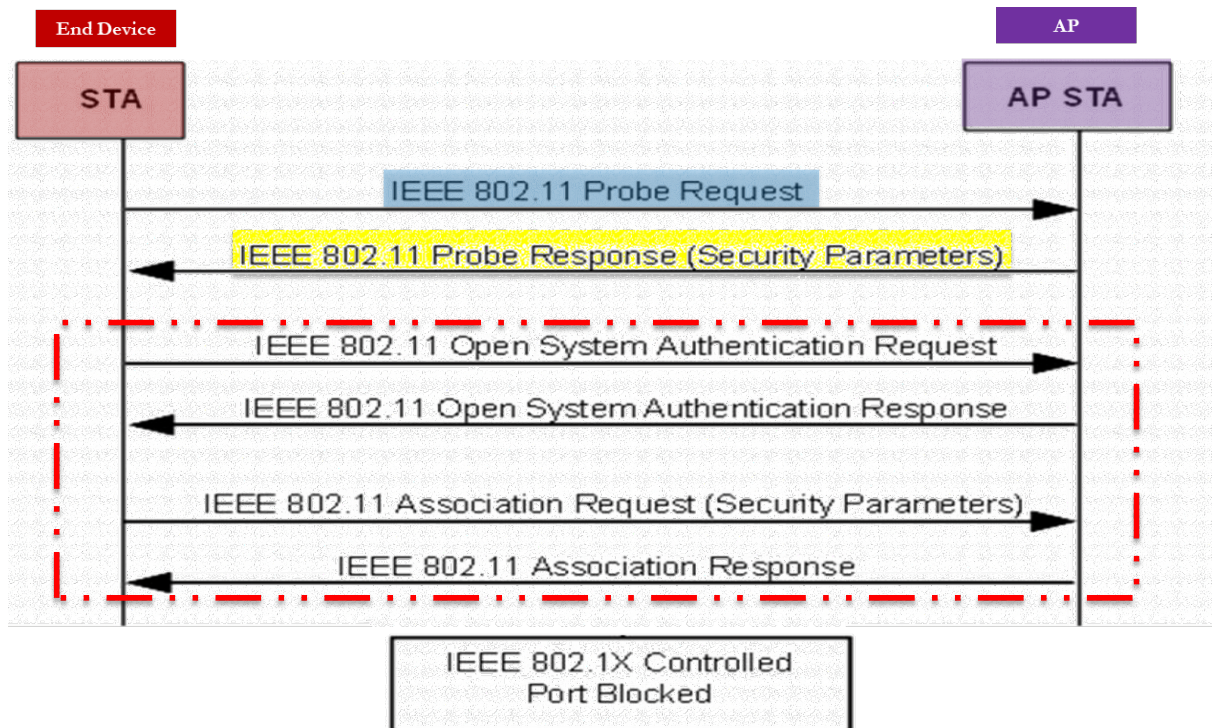


Figure 4-17—Establishing the IEEE 802.11 association

281. As I explained in claim 4, *Vardi* teaches or at least renders obvious this connection procedure, identified in *Vardi* by “IEEE 802.11 association procedure” a “sequence of steps” for “establishing a WiFi connection to the Internet.” See X.4

282. For example, explains that the mobile device and AP perform an “IEEE 802.11 association procedure” to establish connection. 7:36-40 (“establishing a WiFi connection to the Internet requires a **sequence of steps**, starting with the **IEEE 802.11 association**, continuing with security exchange, essential network IP information acquisition and accessing specific network location.”), 10:34-35 (“F1—

Basic **IEEE 802.11 association procedure (inclusive of WEP, if needed)**”), 50
 (“F2—IEEE 802.11 authentications, (WPA, WPA2...)”)

283. *Vardi*, teaches or at least renders obvious this connection procedure, identified in *Vardi* as “IEEE 802.11 association.” Ex. 1007, 7:36-40, 10: 34-53 (“F1—Basic IEEE 802.11 association procedure (inclusive of WEP, if needed); either using beacon information or probing to get association information.”).

284. As I explain in the background section, there are three major 802.11 connection procedure steps: (1) device discovery (scanning); (2) device authentication (checking capability); and (3) establishment of connection (association). Corresponding to the three connection procedure steps, there are three corresponding connection states: (1) not authenticated or associated; (2) authenticated but not yet associated; and (3) authenticated and associated.

285. *Vardi*, like that of the ’552 patent, presumes knowledge of the 802.11 standard. Thus, a POSITA would have readily understood that *Vardi*’s disclosure referencing “IEEE 802.11 association” knows this disclosure corresponds to *IEEE802.11* Figure 4-17 (below). And that “establishing a WiFi connection to the Internet requires a sequence of steps, starting with the IEEE 802.11 association, continuing with security exchange, essential network IP information acquisition and assessing specific network location.” Ex. 1007, 7:36-43.

286. *Vardi* also describes these three states as “F1—Basic IEEE 802.11 association procedure (inclusive of WEP, if needed); either using beacon information or probing to get association information.” Ex. 1007, 10:34-39. A mobile device must be authenticated and associated for data transfer (Internet connection).

287. In my opinion, a POSITA would have readily understood that to “establish[] a WiFi connection...starting with the IEEE 802.11 association” is inclusive of Limitation 8[h] as defined by *IEEE802.11*.

288. But even if I assume that a POSITA does not have this working knowledge, *Vardi* explicitly directs a POSITA to *IEEE802.11* for the underlying implementation of the “IEEE 802.11 association procedure.”

289. As shown below, *IEEE802.11* Figure 4-17 illustrates this procedure for an “Open System” authentication and association.

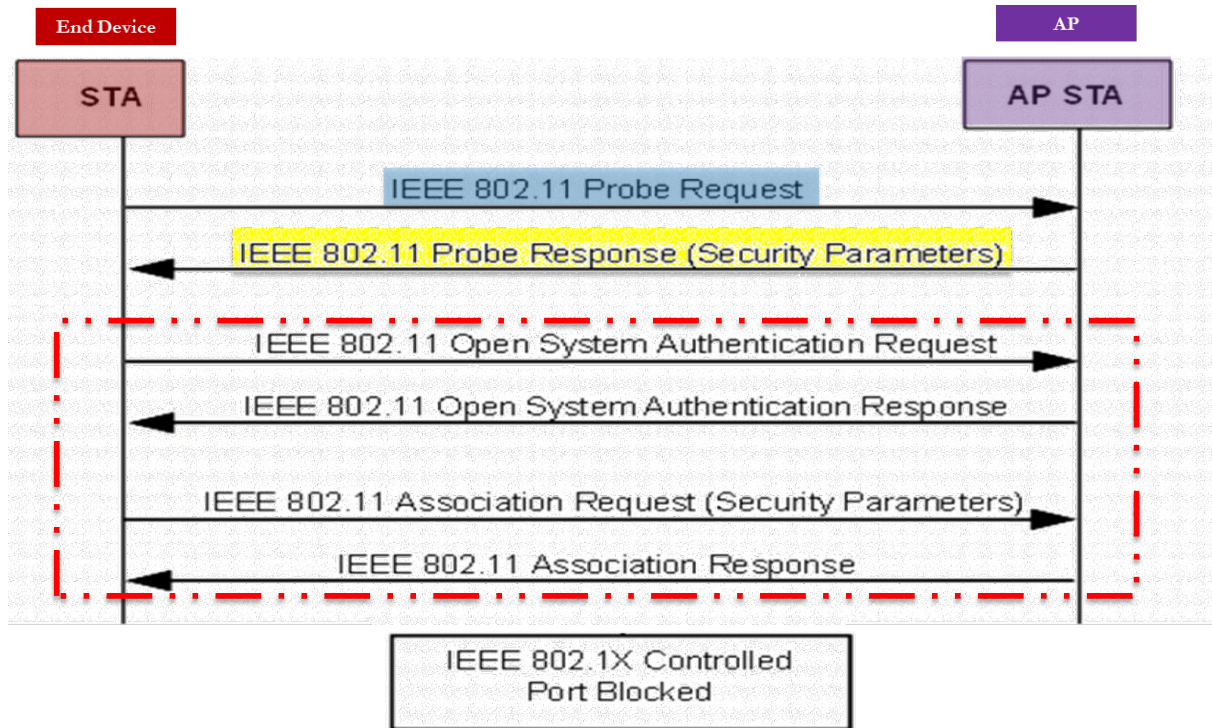


Figure 4-17—Establishing the IEEE 802.11 association

290. Thus, even if *Vardi* does not provide the underlying details of the connection procedure, which I believe it does to a POSITA, *Vardi* in view of *IEEE802.11* illustrates the connection procedure between the mobile device and AP in Figure 4-17 (shown above).

291. That is, *IEEE802.11* defines the connection procedure between a mobile device (“STA”) and an AP (“AP STA”). *IEEE802.11* illustrates that after the mobile device and AP exchange probe request and response frames, the mobile device transmits an authentication request frame, and the mobile device receives the

AP's transmitted authentication response frame, at which point the mobile device and AP are connected. Next, the mobile device transmits an association request frame, and the mobile device receives the AP's transmitted association response frame, at which point the mobile device is authenticated and associated.

292. A POSITA would have naturally looked to *IEEE802.11* to provide the underlying implementation details of *Vardi's* connection procedure and found it obvious to do so. *See I.A.*

293. *IEEE802.11* dictates that a "STA shall be able properly to construct a subset of the frames specified in this clause for transmission and to decode... All STAs shall be able to validate every received frame... and to interpret certain fields from the **MAC headers** of all frames." *IEEE802.11*, 380. *IEEE802.11* further explains that "[e]ach frame consists of the following... *MAC header*... A variable-length *frame body*, which contains information specific to the frame *type* and *subtype*..." *IEEE802.11*, 380 (emphasis in original). *IEEE802.11* sets forth the general frame format, which includes a **MAC header** and **frame body**. *IEEE802.11*, 8.2 MAC frame formats.

294. The "MAC frame format comprises a set of fields that occur in a fixed order in all frames. Figure 8-1 depicts the general MAC frame format." While Figure 8-2 identifies, for example, "The Type and Subtype fields together identify the function of the frame." Thus, as identified in Table 8-1 of *IEEE802.11*, fields

“Type and Subtype” identify whether the communication is an “Association request,” “Association response,” “Probe request,” “Probe response,” or “Authentication,” which are transmitted with the MAC header. And the MAC header includes the MAC address—claimed authentic device identifier—during the connection request.

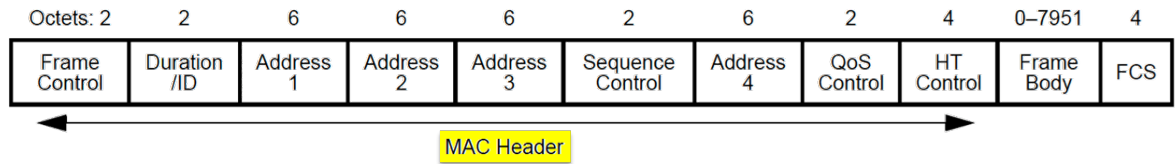


Figure 8-1—MAC frame format

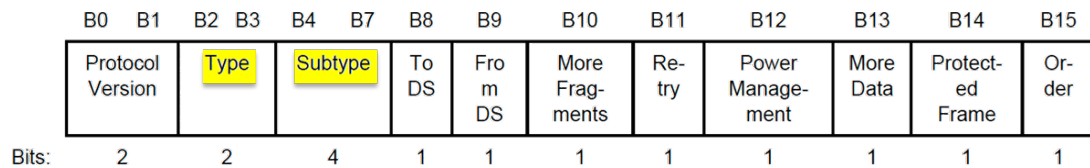


Figure 8-2—Frame Control field

Table 8-1—Valid type and subtype combinations

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110	Timing Advertisement

Table 8-1—Valid type and subtype combinations (continued)

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication

295. As shown below, after the device discovers and selects the “preferred AP,” it performs an exchange comprising at least four frames (shown in the red dotted box). *IEEE802.11* expressly discloses that the MAC address—authentic device identifier—is transmitted as part of each message Type and SubType for connection.

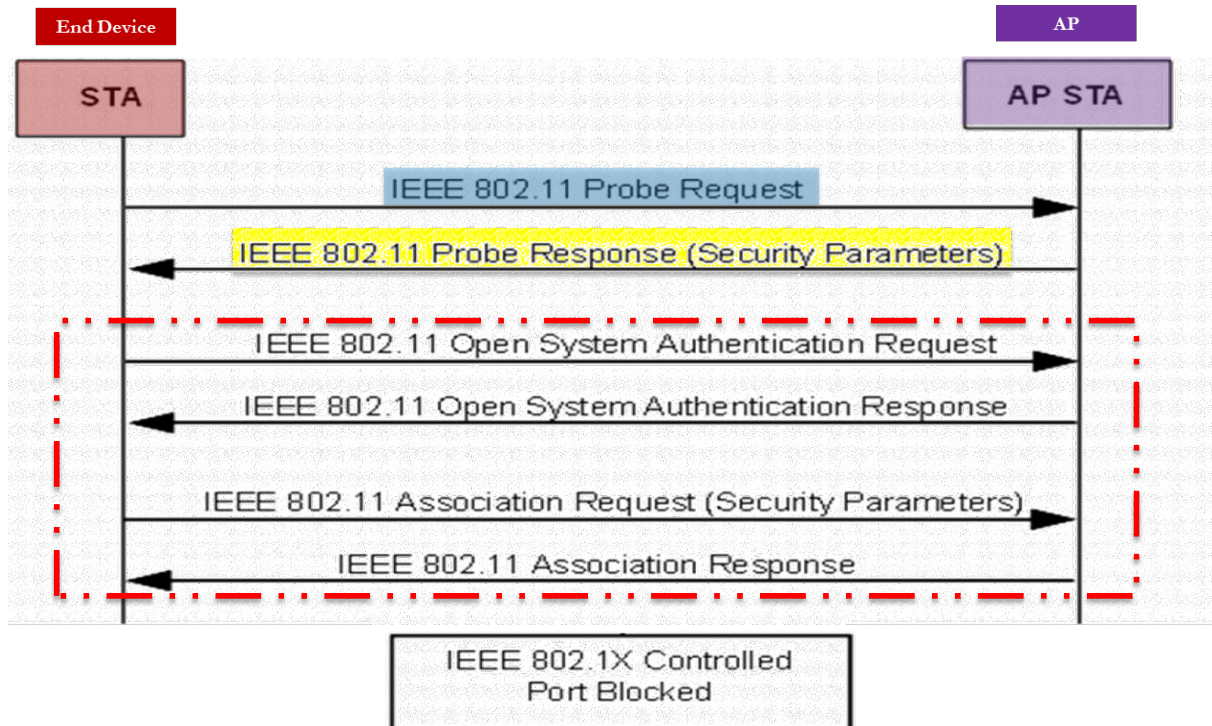


Figure 4-17—Establishing the IEEE 802.11 association

8.2.4.3.5 DA field

The DA field contains an IEEE MAC individual or group address that identifies the MAC entity or entities intended as the final recipient(s) of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field.

8.2.4.3.6 SA field

The SA field contains an IEEE MAC individual address that identifies the MAC entity from which the transfer of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field was initiated. The individual/group bit is always transmitted as a 0 in the source address.

8.2.4.3.7 RA field

The RA field contains an IEEE MAC individual or group address that identifies the intended immediate recipient STA(s), on the WM, for the information contained in the frame body field.

8.2.4.3.8 TA field

The TA field contains an IEEE MAC individual address that identifies the STA that has transmitted, onto the WM, the MPDU contained in the frame body field. The Individual/Group bit is always transmitted as a 0 in the transmitter address.

8.2.3 General frame format

The MAC frame format comprises a set of fields that occur in a fixed order in all frames. Figure 8-1 depicts the general MAC frame format. The first three fields (Frame Control, Duration/ID, and Address 1) and the last field (FCS) in Figure 8-1 constitute the minimal frame format and are present in all frames, including reserved types and subtypes. The fields Address 2, Address 3, Sequence Control, Address 4, QoS Control, HT Control, and Frame Body are present only in certain frame types and subtypes. Each field is defined in 8.2.4. The format of each of the individual subtypes of each frame type is defined in 8.3. The components of management frame bodies are defined in 8.4. The formats of management frames of subtype Action are defined in 8.5.

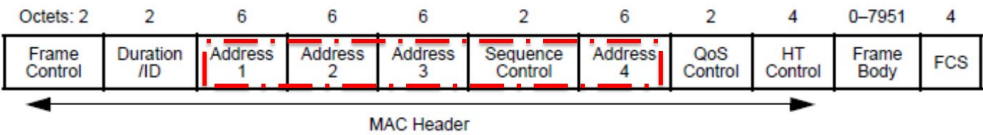


Figure 8-1—MAC frame format

296. A POSITA would have found it obvious to review the underlying implementation providing by the *IEEE802.11* standard to establish a connection of its mobile device to the network.

6. Claim 6

Claim 6	The method of claim 5, wherein the access point includes a Wi-Fi access point, and wherein the communication network includes a Wi-Fi network.
---------	--

297. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 6.

298. As I explained in claim 2, in my opinion, *Vardi* teaches this claim. See *X.2*.

299. *Vardi* teaches that the APs provide Wi-Fi (e.g., wireless Internet access). Ex. 1007, 14:66-15:1 (“In FIG. 3, a computing resource, such as server **310**, and radio access points **370 a-d** are connected to a network **305**, such as the Internet. In

this embodiment, access point **370 d** belongs to a user who also uses access device **320**, such as a laptop, a PDA, etc. The user generally is able to access the Internet **305** by connecting device **320** to access point **370 d** wirelessly.”)

300. Additionally, *Vardi* explains that the mobile devices communicate with the APs via Wi-Fi standards and enabled components. Ex. 1007, 9:54-59 (“clients continuously collect radio resources information about APs detected by the wireless user terminal. These clients can be executed on laptops, handheld devices (PDA[s]), cellphones, or any other devices that incorporates a radio facility for wireless communication, such as *WiFi*.”); 5:11-16 (“Wifi enabled mobile telephones”).

301. Further, FIG. 3 of *Vardi* illustrates a mobile device in wireless communication with APs connected to the Internet 305.

7. Claim 7

Claim 7	The method of claim 4, wherein the access point was previously communicatively coupled with the device.
---------	---

302. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 7.

303. *Vardi* discloses “the access point was previously communicatively coupled with the device.” Ex. 1007, 13:4-23, 14:52-57.

304. *Vardi* details a selection process for mobile devices favoring “previously communicatively coupled” access points.

305. *Vardi* explains that the mobile device and ‘favorite’ AP was “previously communicatively coupled,” and the mobile device takes advantage of that knowledge when connecting. *Id.*, 13:4-23.

306. Specifically, *Vardi* describes, “[i]f a ‘favorite’ AP (AP is called favorite if it is *part of radio resource database* that had been distributed to client...) is detected by the IEEE 802.11 scan... (ex. Owner’s AP), the client can select this AP for connection.

307. That is, *Vardi*’s mobile device executes an IEEE 802.11 active scan by sending out a probe request frame to neighboring APs, the neighboring APs respond with their probe response frames, including their SSID—here “favorite”—the mobile device compares the SSID within its memory to the received access point information—SSID: “Favorite”—and if the two match, they were “previously communicatively coupled” and it “select this AP for connection.” *Id.*, 13:4-23; 14:52-57.

308. *Vardi* details another procedure for connecting to “previously communicatively coupled” APs, explaining, “If a list of previously successfully used access points is available (locally stored) and some APs on the list are available . . . the client can select the AP... for connection.”

309. Again, “some APs on the list” is *Vardi*’s reference to a probe response from the APs nearby providing information about themselves to the mobile device. The mobile device compares and “can select the AP... for connection.” *Id.*

310. “[P]reviously communicatively coupled” APs to mobile devices is a well-known concept. At the time of the alleged invention, it was well-known that mobile devices-maintained lists of “previously communicatively coupled” APs. *Vardi* also discloses the same.

311. Additionally, *Vardi* details speeding up the connection process between mobile devices and APs by exploiting access point connectivity information from “previously communicatively coupled” APs. 7:36-43.

312. *Vardi* describes that the mobile device “connection process will exploit the radio resource information in its memory. Next, the client selects the most favorable access point for connection.” *Id.*, 13:9-12.

8. Claim 8

Claim 8	The method of claim 4, wherein the authentic device identifier includes a media access control (MAC) address of the device.
---------	---

313. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 8.

314. In my opinion, *Vardi* teaches transmitting the MAC address to the AP during “probing.” A POSITA understands “probing” in the context of *Vardi* and

IEEE 802.11 to mean transmitting a probe request and receiving a probe response. It is well-known that IEEE 802.11 probe request/response frames include a MAC header comprising the MAC address of the device (the claimed authentic device identifier includes a MAC address).

315. However, I understand that Patent Owner may argue that *Vardi*'s disclosures are not explicit, and I have been asked to consider whether it alone or in view of additional references—here *IEEE802.11*—renders obvious the authentic device identifier including a MAC address. They do.

316. First, a POSITA would have found *Vardi*'s disclosure at least renders obvious the authentic device identifier comprises a MAC address as explained above.

317. Second, as I explain in the motivation to combine section and background on *IEEE802.11*, a POSITA would naturally look to the standard specification, IEEE 802.11, to further understand and implement the described “IEEE” procedures disclosed by *Vardi*. See Section IX.F.1.

318. *Vardi* explicitly directs a POSITA to read and consider the underlying implementations and details provided by *IEEE802.11*. For example, *Vardi* describes, “IEEE 802.11 association,” “Basic IEEE 802.11 association,” “IEEE 802.11 authentications,” “IEEE 802.11 scan results,” “IEEE 802.11 scan,” and “probing.”

319. These are well-known terms of art in the industry that a POSITA would have readily understood direct you to IEEE 802.11. Particularly, “probing,” “scan,”

and “association.” As shown below, FIG. from IEEE 802.11 depicts the messages of an Active Scan procedure between a mobile device and AP. See Section IX.F.1.

320. Third, a POSITA, in my opinion, would naturally look to *IEEE802.11* specification to supplement their understanding of the requirements to perform *Vardi*’s “IEEE 802.11 association” or “IEEE 802.11 scan” procedures.

321. Looking at *IEEE802.11* it explicitly discloses an Active Scan procedure between a mobile device, whereby the mobile device transmits a probe request frame comprising an authentic device identifier, which is the MAC address.

10.1.4.3.3 Active scanning procedure

Upon receipt of the MLME-SCAN.request primitive with ScanType indicating an active scan, a STA shall use the following procedure:

For each channel to be scanned:

- Wait until the ProbeDelay time has expired or a PHYRxStart.indication primitive has been received.
- Perform the Basic Access procedure as defined in 9.3.4.2.
- Send a probe request to the broadcast destination address, with the SSID and BSSID from the MLME-SCAN.request primitive. When the SSID List is present in the MLME-SCAN.request primitive, send one or more probe request frames, each with an SSID indicated in the SSID List and the BSSID from the MLME-SCAN.request primitive.
- Set to 0 and start a ProbeTimer.
- If PHY-CCA.indication (busy) primitive has not been detected before the ProbeTimer reaches MinChannelTime, then set NAV to 0 and scan the next channel, else when ProbeTimer reaches MaxChannelTime, process all received probe responses.
- Set NAV to 0 and scan the next channel.

See Figure 10-3.

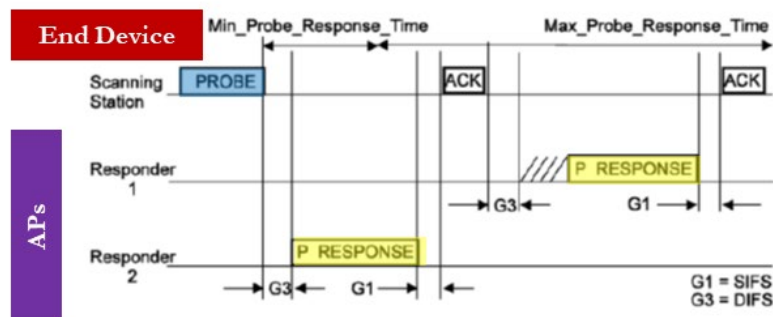


Figure 10-3—Probe response

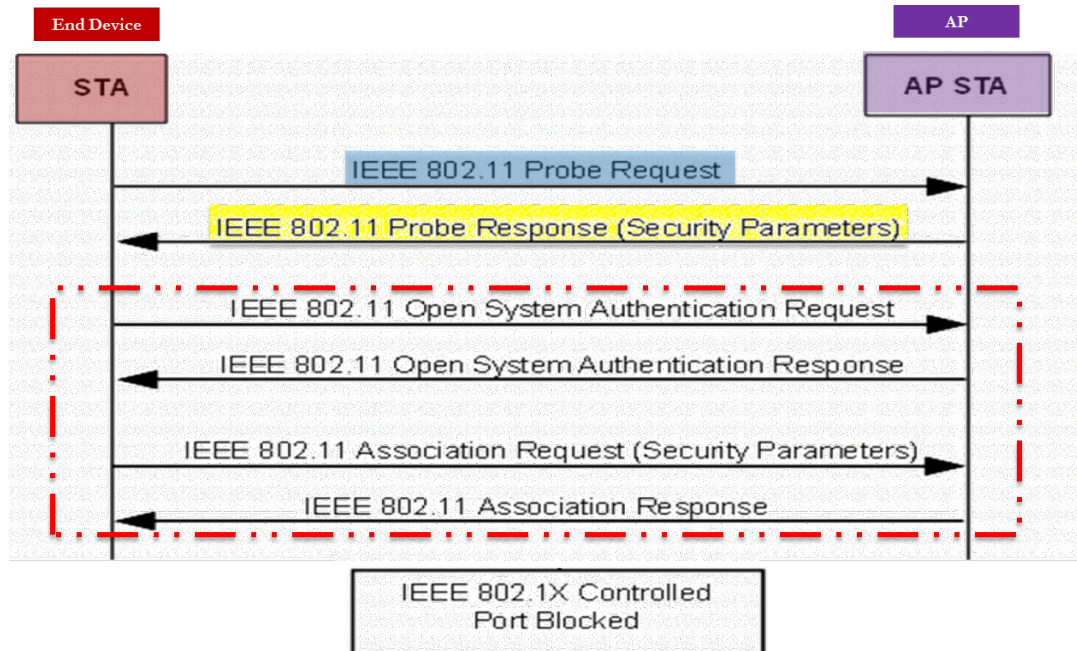


Figure 4-17—Establishing the IEEE 802.11 association

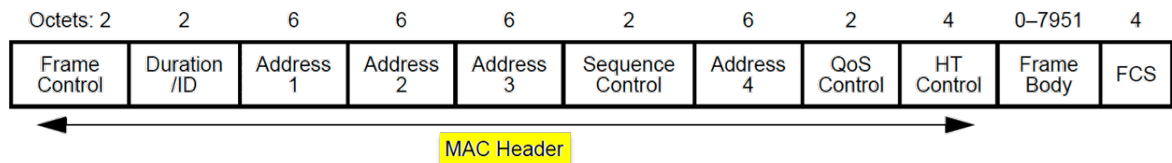


Figure 8-1—MAC frame format

9. Claim 9

Claim 9 The method of claim 4, wherein the information regarding the access point includes at least one of a media access control (MAC) address of the access point or a service set identifier (SSID) of the access point.

322. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 9. See limitation 4[b] (§X.4.iii).

323. *Vardi* describes the access point information comprises the SSID (referred to in *Vardi* as “Network name”) and MAC address:

i. Network name;	xii. User Terminal Location;
ii. MAC address;	xiii. Access Point Location;
iii. Received signal strength and variance over time;	xiv. Mapping Type—how an access point location was determined.
iv. Encryption status;	The data base of data can comprise the above information as well as:
v. Internet connection available capacity;	i. Location
vi. Access protocol response times;	ii. Internet accessibility
vii. Gateway IP address;	iii. Long term behavioral statistics comprising:
viii. DNS address;	Percentage of availability
ix. Occupied IP addresses;	Signal strength variance
x. Captive portal credentials;	Available bandwidth
xi. Connection Technology;	iv. Name of owner;
	v. Owner profile;
	vi. Password.

324. And *IEEE802.11* defines a probe response frame including a MAC Header and frame body , which comprises the MAC address and SSID of the AP:

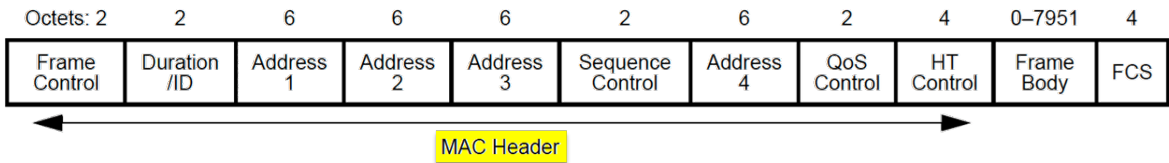


Figure 8-1—MAC frame format

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 8.4.2.2.
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set element is present within Probe Response frames generated by STAs using FH PHYs.

⋮

Order	Information	Notes
23	Measurement Pilot Transmission	The Measurement Pilot Transmission element is present if dot11RMMeasurementPilotActivated is between 2 and 7.
24	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RMMeasurementPilotActivated is between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 10.11.14) with two or more members, or if dot11MgmtOptionMultiBSSIDActivated is true, or if dot11InterworkingServiceActivated is true and the AP is a member of a Multiple BSSID Set with two or more members and at least one dot11GASAdvertisementID MIB attribute exists.

XI. *VARDI*, *IEEE802.11*, *ORAVA* AND *YUN* RENDER CLAIMS 10-28 OBVIOUS

A. Obviousness of Claims 10-28 (IPR2024-01369 Ground 1)

1. Independent Claim 10

325. In my opinion, *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 10.

i. Limitation 10[pre]:

10[pre] A method performed by a device, the method comprising:

326. I understand that the preamble of claim 10 merely states the purpose or intended use of the claimed subject matter, which is not limiting.

327. *Vardi* teaches a wireless communication system where the user terminal performs a method for connecting to the Internet via an access point using access point information (“API”) it received from the server. Ex. 1007, 3:11-13.

328. *Vardi* describes an “inventive method and system...” *Id.*, 6:49-54.

329. *Vardi* explains “a method for enhancing connectivity to radio access points.” 4:18-27.

ii. Limitation 10[a]:

10[a]	receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
-------	---

330. The asserted patents do not define an “authenticated access point list” nor is it a term of art, however, FIG. 2 of the asserted patents “shows an illustrative example of an authenticated access point list.”⁶ And the corresponding disclosure for FIG. 2 indicates that an “authenticated access point list” may include a SSID or a MAC address. Ex.1001, 4:37-45.

331. Patent Owner’s (PO) infringement contentions add that the SSID and the MAC address are of previously connected access points. Ex1011, 22.

⁶ I have been asked, for purposes of this proceeding, to assume the term is definite.

332. *Vardi* teaches an “authentic access point list” that includes SSIDs and MAC addresses for both previously connected APs and newly discovered APs. Ex. 1007, 3:4-6, 25-54, 12:35-39.

333. *Vardi* describes a communication system where the mobile device gather access point information (API) from nearby APs, transmits that gathered API to a server, where the server stores the received information in one or more databases, and then transmits the API to the mobile device for storing. *Id.*, 3:4-6.

334. Specifically, *Vardi* explains that “clients receive updates about relevant access points from the server and use the information to select and connect to the preferred access point.” *Id.*, 3:4-6.

335. *Vardi* explains that the access point information “can include access connectivity information that can be used by the wireless user terminal to connect to the access point.”

336. And *Vardi* provides, as shown below, a listing of API that is included.

- i. Network name;
- ii. MAC address;

- iii. Received signal strength and variance over time;
- iv. Encryption status;
- v. Internet connection available capacity;
- vi. Access protocol response times;
- vii. Gateway IP address;
- viii. DNS address;
- ix. Occupied IP addresses;
- x. Captive portal credentials;
- xi. Connection Technology;

- xii. User Terminal Location;
 - xiii. Access Point Location;
 - xiv. Mapping Type—how an access point location was determined.
- The data base of data can comprise the above information as well as:
- i. Location
 - ii. Internet accessibility
 - iii. Long term behavioral statistics comprising:
 - Percentage of availability
 - Signal strength variance
 - Available bandwidth
 - iv. Name of owner;
 - v. Owner profile;
 - vi. Password.

337. Regardless whether the API is for previous connections or new connections, *Vardi* teaches it.

338. For previous connections, *Vardi* describes that “[i]f a ‘favorite’ AP (AP is called favorite if it is part of radio resource database that had been distributed to client)... is detected by the IEEE 802.11 scan... the client can select this AP for connection...” *Id.*, 13:13-17.

339. That is, the mobile device performs a scan for neighboring APs, the neighboring APs respond, the mobile device compares the API stored from the server with the information from the APs response and determines whether “‘favorite’ AP” (the SSID of a previously connected AP) is the same SSID returned from the scan. Here, as *Vardi* describes, it is then the mobile device “select this AP for connection.” Ex. 1007, 13:13-17.

340. Moreover, saving API and connecting to a preferred AP based on the saved AP is well-known to a POSITA at the time of the alleged invention. Ex. 1007, 12:24-30.

341. *Vardi*, confirms the same, stating “it is well known in prior art computing systems to cache information related to an access point to which the mobile device has connected before. . . when the mobile device is activated at a later time in the same locale, the system uses the information in the cache to automatically reconnect to that AP. The cache normally includes the name and the MAC address of the AP.” *Id.*

342. *Vardi* teaches mobile devices “executes a program (e.g., a client) that uses the combined data to find usable radio resources or wireless APs and establishes network connections through them, for example connections to the internet.” *Id.*, 7:10-14.

343. *Vardi* also teaches about the server transmitting API for APs the mobile devices have not connected to previously. Ex. 1007, 12:30-39 (“when the mobile device is activated in a new location, it **has no information in the cache** to enable fast connection to an AP... the **server sends cache information to each client, relating to all APs** in the vicinity of the client... In this manner, the mobile device can have cache information of APs to which the mobile device **was not connected before.**”).

344. Thus, in my opinion, regardless of whether an “authenticated access point list” includes SSIDs or MAC addresses for previously connected APs or new ones, *Vardi* teaches it.

345. The asserted specifications also do not define “controlled by the server.” Ex. 1001. The only reference to “controlled by the server” in the specification of the ’552 patent is to indicate that “the authenticated access point may include an access point controlled by mobile operating server.” Ex. 1007, 4:33-35.

346. But reviewing the claims, claim 24 adds that “wherein to determine the... access point is... under control of the server, the determination unit determines whether the information regarding the... access point is *included in the authenticated access point list*.” Ex. 1001, cl. 24.

347. Thus, claim 24 indicates that APs are under the server’s control if they are “included in the authenticated access point list.” Ex1001, cl. 24.

348. *Vardi* discloses that the mobile device determines whether the AP is the preferred AP—an authenticated access point—by comparing the stored API (APs on the list under server control) with the API received from an *IEEE802.11* scan.

349. When client becomes active it executes an IEEE 802.11 scan for APs in reach and determines the SSID, MAC address... Using the MAC address, the client can compare this scan result with its radio resource database to determine which APs are preferred for connection...” Ex. 1007, 14:52-57.

350. That is, *Vardi* describes that the “radio resource database” is the stored access point information receive from the server. The mobile device compares the scan results, a POSITA understand the scan is a probe request and the results are a probe response, which includes the SSID and MAC address of the APs that responded. If an AP is not on the list, it is not under control of the server, however, if the AP is on the list, it is under control of the server. Ex. 1001, cl. 24.

351. *Vardi* teaches or at least renders obvious that the APs are controlled by the server.

352. I have been asked to consider alternative positions PO may contend. One position, if PO contends that contends that controlled by the server means that the server can engage in a request-response interaction with the AP.

353. In my opinion, if PO contends that a request-response interaction is the definition of controlled by the server, *Vardi* teaches that as well.

354. *Vardi* describes that the “[s]erver can also include an evaluation module, which can *evaluate[] accessibility, bandwidth and other characteristics of various AP[s]*, and store the information as an update in database...” Ex. 1007, 7:53-58. Subsequently, the server transmits this information to the mobile device.

355. *Vardi* further explains that the “*server* can include MappingType information that indicates the method by which the AP was mapped... where the *server* or the client *receives information about the location of an AP using two or*

more different methods of mapping, location determination using one method can be selected to take precedence...” Ex. 1007, 16:47-54.

356. Under this definition, a POSITA would have readily understood *Vardi* disclosure to mean the server request “MappingType” information and the APs respond with the requested “MappingType” information.

357. I have been asked to consider PO’s infringement contention theory where PO’s alleges the probe request-response frames correspond to an AP “controlled by the server.”

358. *Vardi* teaches or at least renders obvious the same probe request-response communication depicted in PO’s infringement contention theory, including the SSID and MAC address. Ex. 1007, 10:25-36, 7:10-46, 9:54-64.

359. *Vardi* explains the mobile device can perform a “Basis IEEE 802.11 association procedure... using... probing to get association information” and “information acquired as part of the standard 802.11 scan, i.e.[,] Network or AP name (SSID—service set identifier); and, AP Radio Mac address” is included in the response from the AP. Additionally, under PO’s infringement theory, *Vardi* teaches or at least renders obvious that the APs are under control of the server because, the “information” about the “relevant access points” is used by *Vardi*’s mobile device to perform a “Basic IEEE 802.11 association procedure... using probing to get

association information” and “connect to the preferred access point.” Ex. 1007, 10:34-36, 3:4-7.

360. Because *Vardi* presumes a POSITA has working knowledge of IEEE 802.11, it does not provide the underlying details. However, a POSITA at the time of the alleged invention, would have readily understood that “IEEE 802.11 association procedure... using... probing” to mean the mobile device issuing a probe request and the AP, in response, issuing a probe response.

361. This is particularly true, here, where *Vardi* provides additional disclosures related to “IEEE scan” and “IEEE association.”

362. Ex. 1007, 10:25-28 (For example, “AP security status (e.g., WEP, WPA, WPAII)” “information can be tagged or association with information acquired as part of the standard 802.11 scan, i.e.: Network or AP name (SSID—service set identifier); and, AP Radio MAC address.”), 11:35-36 (“Select local usable wireless connections from IEEE 802.11 scan results.”), 12:17-20 (“when the AP is already part of radio resource database, only F1 (association), F2 (WPA exchange) and F4 are needed, thereby substantially reducing the average connection”), 13:4-7 (“Connecting to a wireless network starts by scanning the neighborhood for candidate AP connections (IEEE 802.11 scan). The IEEE 802.11 scan can produce a list of access points in reach.”).

363. These additional disclosures inform a POSITA that *Vardi*'s "IEEE 802.11 scan" and "IEEE 802.11 association procedure" encompass IEEE 802.11 "Active Scan." Thus, *Vardi* teaches or at least renders obvious PO's infringement contention theory.

364. Even if PO's contends that a POSITA would not have found *Vardi*'s disclosures of "probing," "IEEE 802.11 scan," and "IEEE 802.11 association procedures" explicit, a POSITA would have naturally looked to *IEEE802.11* to supplement its understanding of *Vardi*'s "IEEE 802.11 scan" and "IEEE 802.11 association procedure" because *Vardi* directs a POSITA to *IEEE802.11*.

365. *IEEE802.11*'s disclosure is explicit. See *IEEE802.11*, Figure 4-17.

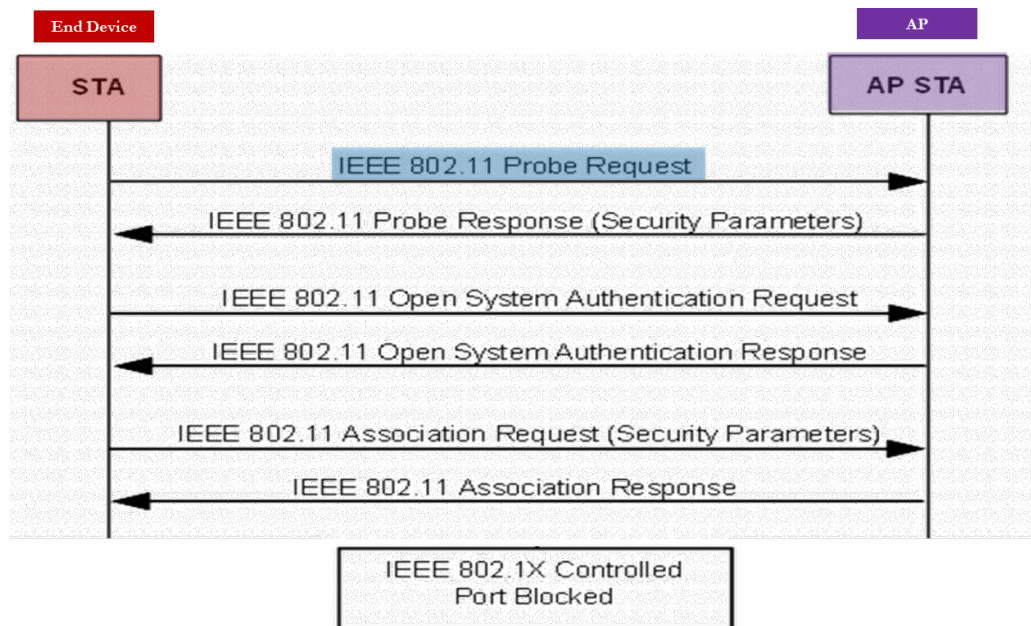


Figure 4-17—Establishing the IEEE 802.11 association

366. I have also considered whether the additional prior art references teach or render obvious APs “controlled by the server.”

367. In my opinion, *Orava* explains that the server assigns MAC address to the access points. Ex. 1005, ¶[54] (“In a server of the network, for example in the [] PAC, a list can be maintained to which the temporary MAC addresses allocated by the different access points AP are added. Thus, the AP can transmit a request for allocation of a temporary MAC address. On the basis of the request, the server selects an available address and transmits a response frame comprising the allocated address MAC.”).

368. That is, address assignment demonstrates that the server controls the AP.

369. A POSITA would have found it obvious to combine the underlying implementation details of *IEEE802.11* and *Orava*’s server management capabilities to *Vardi*’s server. See Section IX.F.1.

370. First, both *Vardi* and *Orava* are built on top of *IEEE802.11* and thus, a POSITA would have known the standard aid in interoperable systems. See Section IX.F.1.

371. Second, a POSITA would have a likelihood of success as *Vardi* and *Orava* explicitly directs a POSITA to use *IEEE802.11*. Standards are meant to provide a reliable basis for people to share expectations, here, wireless connectivity.

372. Third, *Vardi* and *Orava* disclose a multi-AP system enabling connections between mobile devices, APs, and the Internet. A POSITA would have found it obvious to add *Orava*'s central server management capabilities, controlling the APs, to *Vardi*'s server because a POSITA would have understood the need to manage and distribute access point configurations within the system, for example, utilizing a single "SSID" for the "access points 370a-d."

373. A well-known example is moving through an office building, there a user's mobile device is connected to the SSID ("Office") despite as the user moves floors connecting to a different access point. The APs are "controlled by the server," where the server issues the same SSID for numerous APs. *IEEE802.11* ("4.3.13.12 Multiple BSSID capability – Multiple BSSID capability enables the advertisement of information for BSSIDs using a single Beacon or Probe Response frame instead of multiple Beacon and Probe Response frames, each corresponding to a single BSSID.")).

374. Moreover, *Orava*'s server management capabilities ensures that the randomly generated Fake IDs will be unique across APs by allocating specific MAC address space per AP. Ex. 1005, ¶[54] ("In a server of the network... a list can be maintained to which temporary MAC address allocated by the different [] AP are added... the server selects an available address and transmits a response..."). See Section IX.F.1.

375. In my opinion, a POSITA would have found it obvious to combine the teachings of *Vardi*, *IEEE802.11*, and *Orava* because their teachings align. See Section IX.F.1.

iii. Limitation 10[b]:

10[b]	receiving, from the server, a fake device identifier for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame;
-------	--

376. *Vardi* teaches IEEE 802.11-standard compliant probing, which transmits a MAC address in the probe request frame to the AP and, in response, the AP transmits a probe response comprises its SSID, MAC address, and numerous other fields defined in IEEE 802.11. But *Vardi* does not teach generating “a fake device identifier” for use in the probe request frame. *Orava* does.

377. *Orava* explains that mobile device generates a REF identifier that it transmits to a central server (referred to as PAC) where the central server or PAC generates a random fake device identifier and then, in response to the mobile device’s message, transmits the fake device identifier for use by the mobile device for “all protocol messages.” Ex. 1005, ¶¶[26], [32], [34], and [49].

378. *Orava* explains two embodiments for the server generating the fake device identifier both teach this limitation and both are compatible with each other. Ex. 1005, ¶[26].

379. *Orava* teaches that “MT transmits a request comprising the identifier it has determined to a second device to arrange a temporary MAC address. The second device may be a second terminal MT, an access point AP or a public access controller PAC, depending on the configuration of the system... On the basis of the request, a **temporary MAC address MAC**⁷ can be arranged in the second device to be used... The second device transmits a response frame relating to the arrangement of the MAC address comprising an identifier (MAC/REF). The MT identifies on the basis of the identifier that the response frame is intended for it. On the basis of the response frame, if the MAC address has been successfully allocated, the terminal MT can start using the MAC address allocated to it...,” the first option.

380. Additionally, *Orava* explains, that “the second device allocates a temporary MAC address MAC on the basis of the request... the identifier mentioned in step 202 is a particular reference identifier REF, which is only used to request 203 for allocation of a MAC address and to respond to it in order for the MT being able to recognize that the response frame is intended for it,” the second option.

⁷ *Orava* refers to “MAC” for the generated temporary random MAC address; to avoid confusion, I refer to it as Fake ID.

381. Both teach a mobile device receiving from a server a fake device identifier.

382. *Orava* explains that the “control of temporary MAC addresses may be centralized for instance in a public access controller PAC.” Ex. 1005, ¶[32].

383. *Orava*’s fake device identifier (Fake ID) can be generated utilizing one of a number of methods. *Orava* describes the Fake ID “MAC can be a random number generated by means of a random number generator. MAC can be selected from the address space allocated to the MT on the basis of an address selection algorithm. A temporary MAC address MAC can be allocated to the MT for instance from among organization-specific unique identifiers (OUI) reserved for this purpose. Typically, one OUI allows 2^{24} addresses. The IEEE 802 MAC address format allows locally administrable MAC addresses, in which there are 46 available bits in a 48-bit address format for selecting the temporary MAC address. A MAC address can also be formed of a network identifier, such as a BSS identifier BSSID, and of a random part added thereto, for example.” Ex. 1005, ¶[30].

384. Each of *Orava*’s generation algorithms results in a Fake ID that includes either a random character or number as required by the claim; however, *Orava* details that its Fake ID is generated in “IEEE 802 MAC address format ... in which there are 46 available bits in a 48-bit address format for selecting the temporary MAC address.” *Id.*

385. In my opinion, it would have been obvious to a POSITA to apply the randomly generated MAC address to *Vardi*'s probing message as defined by *IEEE802.11*.

386. As I explain in more detail in Section IX.F.1, a POSITA would have a high likelihood of success adding *Orava*'s random generation capabilities to *Vardi*'s server.

387. *Orava* explicitly informs a POSITA that "MAC" follows the IEEE MAC address format, *IEEE802.11* "allows locally administrable MAC addresses." Ex. 1005, ¶[30].

388. *Orava* teaches that "[p]referably, the use of a temporary MAC address MAC **does not, after arrangement of the address, differ in any way from the use of a fixed MAC address** permanently allocated by the manufacturer. The temporary MAC address can thus be used instead of a fixed address in all protocol messages." Ex. 1005, ¶[49].

389. As detailed above, in my opinion, *Vardi* discloses transmitting an IEEE 802.11 probe request frame. It was well-known at the time of the alleged invention that the IEEE 802.11 probe request frame normally included the "real" MAC address. *See* Ex. 1001, 3:4-18 (describing the alleged problem with IEEE 802.11 "the end device may transmit a probe request frame that may include a device identifier, for the end device such as a media access control (MAC) address of the end device").

390. *Orava* informed a POSITA that “the fixed MAC address determined by manufacturers cause a security risk: a MAC address can be picked up from every message transferred over the air interface...” Ex. 1005, ¶[3].

391. Thus, a POSITA would have found it obvious to swap *Vardi*’s “real” MAC address for *Orava*’s randomly generated Fake ID. Particularly because *Orava*’s Fake ID is in IEEE 802 MAC format, *Orava* instructs a POSITA that use of the Fake ID should not “differ in any way from the use of a fixed MAC address,” and that the Fake ID can be used in “all protocol messages.” Ex. 1005, ¶¶[30], [49]; see Section IX.F.1..

392. As explained above, “real” MAC address are themselves randomly generated and thus, a POSITA would have a high likelihood of success swapping one randomly generated number for another. Particularly true here, where *Orava* generates the Fake ID to remain IEEE 802.11 compliant. See Section IX.F.1.

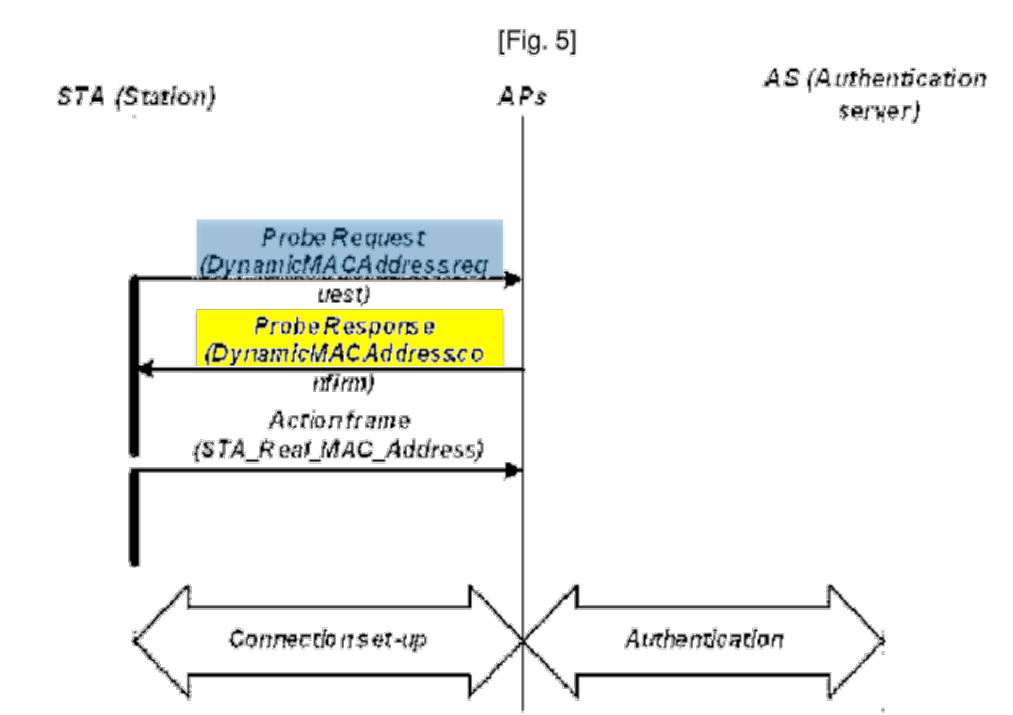
393. The combination requires a simply plug-n-play between the “real” MAC address and the Fake ID randomly generated.

394. In my opinion, the *Vardi-Orava* system is explicit, *Orava* informs a POSITA that the Fake ID can be used in “all protocol messages” and thus, a POSITA would readily have understood that “all protocol messages” includes a probe request. *Yun* confirms my opinion.

395. In considering whether any additional prior art discloses transmitting a Fake ID in the probe request, to the extent that PO contends *Vardi-Orava*'s teachings are not explicit. *Yun* is explicit. *Yun*, Fig. 5, ¶¶[154]-[156].

396. *Yun* explains that “the transmitted packet on air uses an arbitrary MAC address (‘Dynamic MAC address’) which is dynamically allocated.” Ex. 1004, ¶[154].

397. *Yun* further explains “the station(12) transmits the data including the MAC address request such as the probe request(‘Dynamic MAC address request’) to the access points(14).” Ex. 1004, ¶[156].



398. *Yun* explicitly directs a POSITA to using the received generated Fake ID in a “probe request” to have “MAC address anonymity[, which] makes an identity of the station(12) not presumed through the MAC address.”

399. A POSITA would have found it obvious to combine *Vardi*, *Orava*, and *Yun* to transmits the received MAC address (*Orava*) in the probe request frame (*Vardi/IEEE802.11*). See Section IX.F.1.

400. As I explain above, *Vardi*, *Orava*, and *Yun* utilize *IEEE802.11* probe request/response frames to communicate with APs.

401. *Orava*’s Fake ID is formatted as an IEEE802 MAC address and, thus, only requires exchanging one set of characters for another set explaining that the Fake ID can be used the same as the fixed MAC address in “all protocol messages.” Ex. 1005, ¶[49]. And *Yun* explicitly discloses transmitting the Fake ID in the probe request frame. See FIG.5, ¶¶[154-156].

402. If PO contends that *Vardi*, *Orava*, and *Yun* do not explain how a POSITA transmits the Fake ID in a probe request message, neither does the ’552 patent, *IEEE802.11* provides the underlying implementation details. *Vardi*, *Orava*, and *Yun* presume a working knowledge of the *IEEE802.11*, like the ’552 patent, and thus, recognized that a POSITA would understand the workings of “probing,” and transmitting a frame within a “probe message.” As explained above in Section VII

above, the IEEE802.11 probe request frame includes transmitting a MAC address—
(e.g., Address 2)—within the probe request sent by the device to the AP.

10.1.4.3.3 Active scanning procedure

Upon receipt of the MLME-SCAN.request primitive with ScanType indicating an active scan, a STA shall use the following procedure:

For each channel to be scanned:

- Wait until the ProbeDelay time has expired or a PHYRxStart.indication primitive has been received.
- Perform the Basic Access procedure as defined in 9.3.4.2.
- Send a probe request to the broadcast destination address, with the SSID and BSSID from the MLME-SCAN.request primitive. When the SSID List is present in the MLME-SCAN.request primitive, send one or more probe request frames, each with an SSID indicated in the SSID List and the BSSID from the MLME-SCAN.request primitive.
- Set to 0 and start a ProbeTimer.
- If PHY-CCA.indication (busy) primitive has not been detected before the ProbeTimer reaches MinChannelTime, then set NAV to 0 and scan the next channel, else when ProbeTimer reaches MaxChannelTime, process all received probe responses.
- Set NAV to 0 and scan the next channel.

See Figure 10-3.

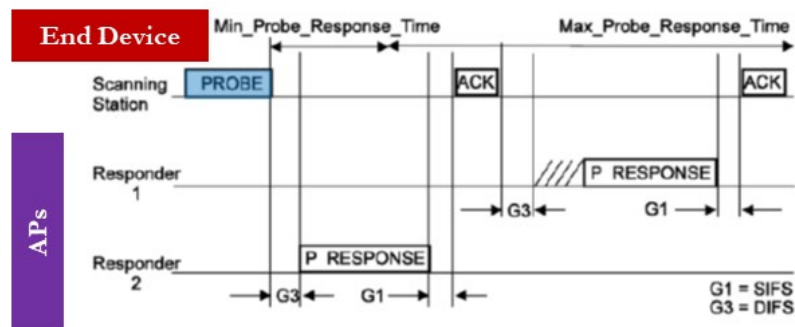


Figure 10-3—Probe response

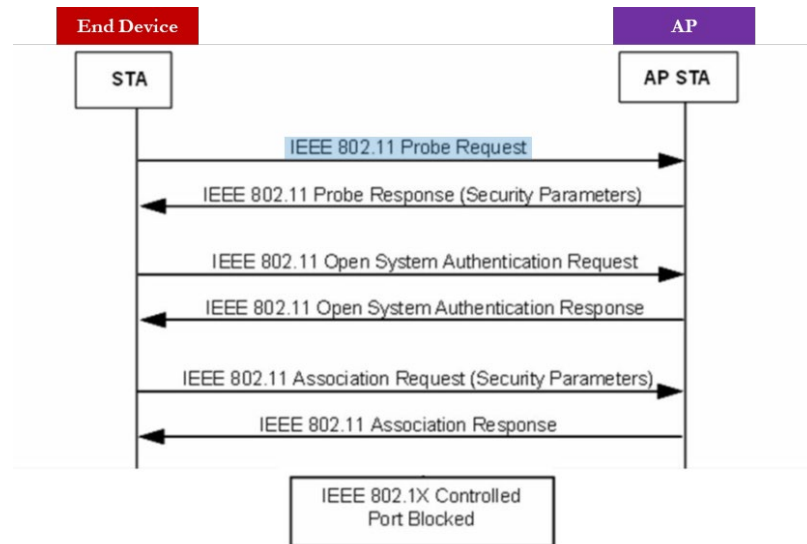
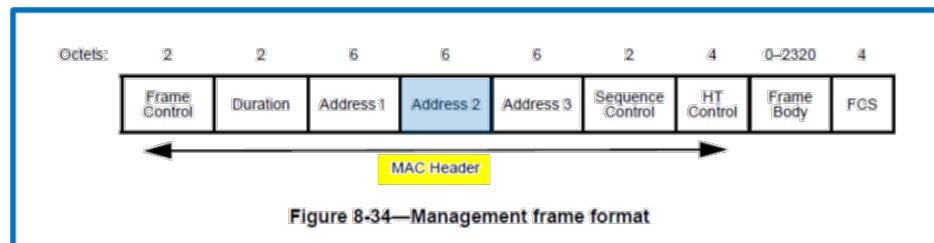


Figure 4-17—Establishing the IEEE 802.11 association



The address fields for all management frames except Multihop Action frames are as follows:

- The Address 1 field of the management frame is the RA (=DA) and is determined as the destination of the frame.
- The Address 2 field of the management frame is the TA (=SA) and is determined as the address of the STA transmitting the frame.
- The Address 3 field of the management frame is set and determined as follows:
 - In management frames of subtype Probe Request, the Address 3 field is the BSSID. The BSSID is either a specific BSSID as described in item 4) below or the wildcard BSSID as defined in the procedures specified in 10.1.4.
 - In management frames of subtype Action, Category Public, the Address 3 field is the BSSID. The BSSID value is set according to 10.19.
 - If dot11OCBAActivated is true, the Address 3 field is the wildcard BSSID.
 - Otherwise:
 - If the STA is contained within an AP or is associated with an AP, the Address 3 field is the BSSID. The BSSID is the address currently in use by the STA contained in the AP.
 - If the STA is contained within an AP or is transmitting the management frame to an AP, the Address 3 field is the BSSID. The BSSID is the address currently in use by the STA contained in the AP.
 - If the STA is transmitting the management frame to one or more members of an IBSS, the Address 3 field is the BSSID of the IBSS.
 - If the STA is a mesh STA, the Address 3 field is the TA.

403. Again, a POSITA would have a high likelihood of success combining *Vardi*, *IEEE802.11*, *Orava*, and *Yun* to plug-n-play the Fake ID (randomly generated in IEEE 802.11 MAC format) for the “real” MAC address (randomly generated) into the 802.11 standard probe request frame. Such a substitute was conventional and well-known at the time of the alleged invention. *See* Section IX.F.1.

iv. Limitation 10[c]:

10[c]	transmitting, to at least one access point, the probe request frame that includes the received fake device identifier;
-------	--

404. As detailed above, *Vardi-IEEE802.11-Orava-Yun* system render obvious the mobile device transmitting a probe request frame including the received Fake ID. *See* limitations 10[a-b] (§XI.A.1.ii-§XI.A.1.iii).

405. The combined system teaches *Vardi*’s mobile device receives a generated random Fake ID from the server, then the mobile device transmits the received randomly generated Fake ID in a probe request frame to the AP. *See* limitation 10[b] (§XI.A.1.iii).

406. Specifically, *Yun* discloses the “***transmitted packet on air uses an arbitrary MAC address*** (‘Dynamic MAC address’)” to provide “MAC address anonymity.”

407. Indeed, *Yun* teaches that the “station(12) transmits the data including the MAC address request such as the probe request(‘Dynamic MAC address request’) to the access points(14).” Ex. 1004, ¶¶[154] - [156].

408. Moreover, in my opinion, a POSITA would have found it obvious to substitute *Vardi*’s “real” MAC address with *Orava*’s Fake ID into *Vardi-IEEE802.11*’s probe request frame (annotated below) because a POSITA would have known it was important to maintain standard compliance as explicitly directed to by each of the references—*Vardi*, *Orava*, and *Yun*.

409. Both *Orava* and *Yun* described the problem with transmitting the “real” MAC address in open messages. Ex. 1005, ¶[3]; Ex. 1004, ¶[154].

410. Naturally, a POSITA would want to protect users’ privacy while also maintaining IEEE 802.11 standard compatibility. *See* Section IX.F.1.

411. And that continuing to use the real MAC address exposed the user to location tracking and privacy concerns.

v. Limitation 10[d]:

10[d]	receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;
-------	--

412. The combination system’s mobile device receives, in response to its probe request, a probe response from neighboring or nearby APs and those probe responses include the SSID and MAC address of the APs as defined per *IEEE802.11*.

413. *Vardi* describes that the mobile device performs a “Basis IEEE 802.11 association procedure... using... probing to get association information” and “information acquired as part of the standard 802.11 scan, i.e.[,]: Network or AP name (SSID—service set identifier); and, AP Radio Mac address” is included in the response from the AP. Ex. 1007, 10:25-36; 13:4-7, 14:52-57, 7:10-46; 9:54-64.

i. Network name;

ii. MAC address;

iii. Received signal strength and variance over time;

iv. Encryption status;

v. Internet connection available capacity;

vi. Access protocol response times;

vii. Gateway IP address;

viii. DNS address;

ix. Occupied IP addresses;

x. Captive portal credentials;

xi. Connection Technology;

xii. User Terminal Location;

xiii. Access Point Location;

xiv. Mapping Type—how an access point location was determined.

The data base of data can comprise the above information as well as:

i. Location

ii. Internet accessibility

iii. Long term behavioral statistics comprising:

Percentage of availability
Signal strength variance
Available bandwidth

iv. Name of owner;

v. Owner profile;

vi. Password.

10.1.4.3.3 Active scanning procedure

Upon receipt of the MLME-SCAN.request primitive with ScanType indicating an active scan, a STA shall use the following procedure:

For each channel to be scanned:

- Wait until the ProbeDelay time has expired or a PHYRxStart.indication primitive has been received.
- Perform the Basic Access procedure as defined in 9.3.4.2.
- Send a probe request to the broadcast destination address, with the SSID and BSSID from the MLME-SCAN.request primitive. When the SSID List is present in the MLME-SCAN.request primitive, send one or more probe request frames, each with an SSID indicated in the SSID List and the BSSID from the MLME-SCAN.request primitive.
- Set to 0 and start a ProbeTimer.
- If PHY-CCA.indication (busy) primitive has not been detected before the ProbeTimer reaches MinChannelTime, then set NAV to 0 and scan the next channel, else when ProbeTimer reaches MaxChannelTime, process all received probe responses.
- Set NAV to 0 and scan the next channel.

See Figure 10-3.

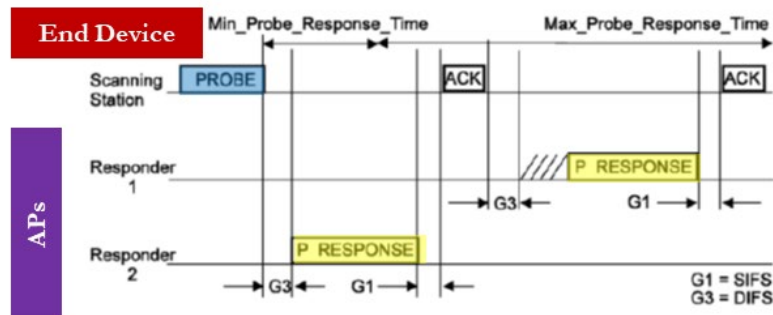


Figure 10-3—Probe response

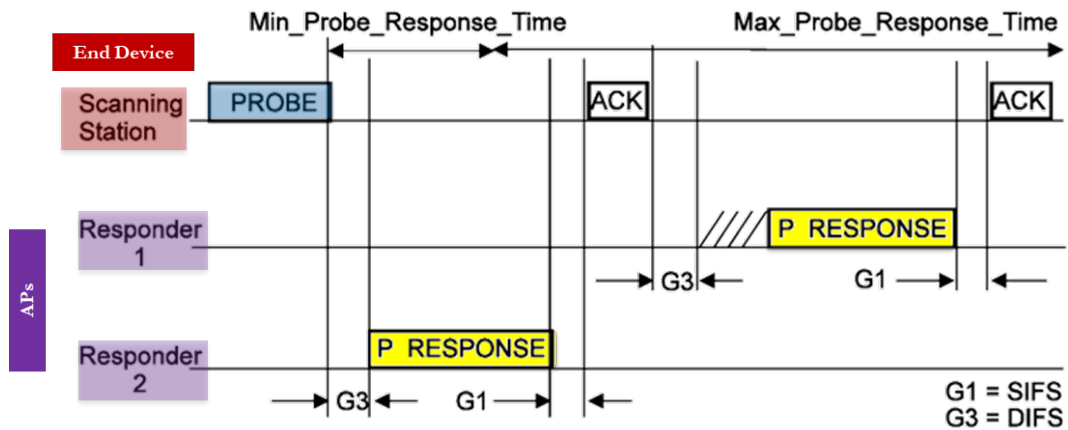


Figure 10-3—Probe response

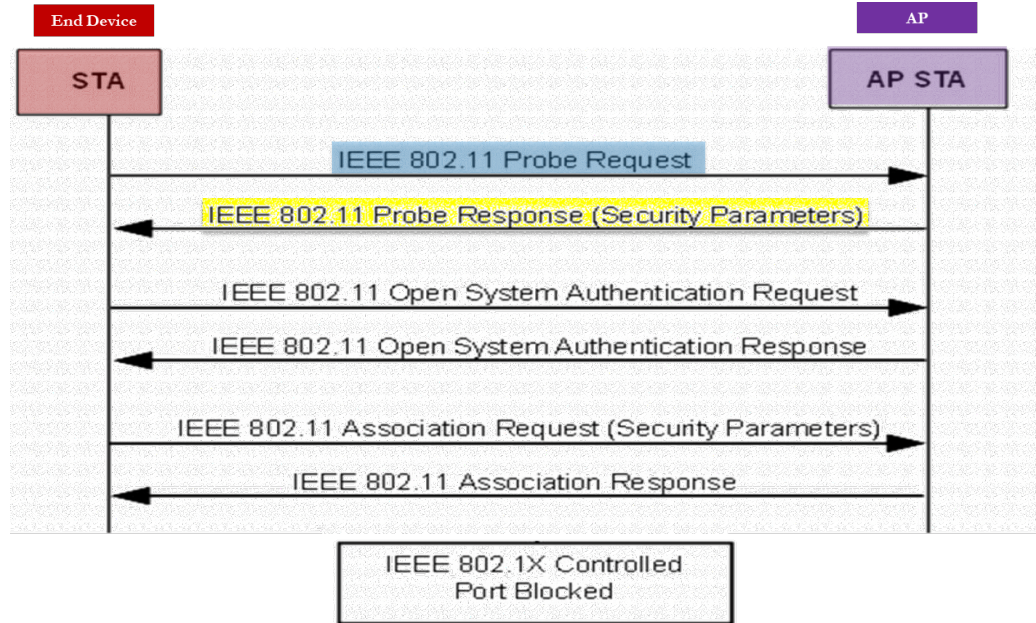


Figure 4-17—Establishing the IEEE 802.11 association

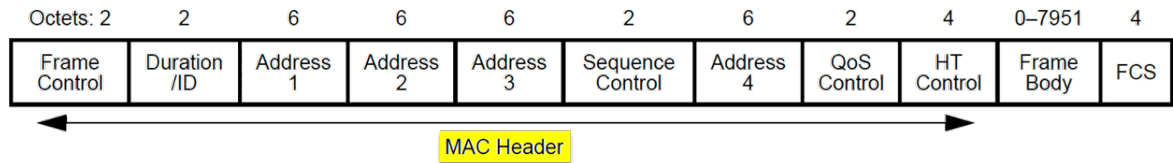


Figure 8-1—MAC frame format

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 8.4.2.2.
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set element is present within Probe Response frames generated by STAs using FH PHYs.

⋮

Order	Information	Notes
23	Measurement Pilot Transmission	The Measurement Pilot Transmission element is present if dot11RMMeasurementPilotActivated is between 2 and 7.
24	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RMMeasurementPilotActivated is between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 10.11.14) with two or more members, or if dot11MgmtOptionMultiBSSIDActivated is true, or if dot11InterworkingServiceActivated is true and the AP is a member of a Multiple BSSID Set with two or more members and at least one dot11GASAdvertisementID MIB attribute exists.

vi. Limitation 10[e]:

10[e] determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server; and

414. *Vardi* teaches that mobile devices store API received from the server in its memory, compare the stored access point information (API) with the API received from an *IEEE802.11* scan to determine whether the AP is the preferred AP—the preferred AP being an authenticated access point—and automatically reconnect to that AP when the mobile device determines that the SSID or MAC address from the *IEEE802.11* scan matches that of the received authenticated access point list stored in memory. *See* limitations 10[a] (§XI.A.1.ii), 10[d] (§XI.A.1.v).

415. *Vardi* explains that “[w]hen client becomes active it executes an IEEE 802.11 scan for APs in reach and determines the SSID, MAC address... Using the MAC address, the client can compare this scan result with its radio resources database to determine which APs are preferred for connection...” Ex. 1007, 14:52-57.

416. That is, *Vardi*’s mobile device performs an “Active Scan,” which as explained above, transmits a probe request frame and receives a probe response frame, the scan results are compared with the previously stored API from the server and the mobile device determines from the comparison whether the probe response API matches the stored API.

417. This procedure of connecting to known or “preferred APs” was well-known. *Vardi* confirms the same. *Vardi* details that “it was well known in prior art

computing systems” for the **devices** to store **API** of previously connected **APs** facilitating **devices** to “automatically reconnect to that **AP**. The cache [memory] normally includes the name and the MAC address of the **AP**.” Ex. 1007, 12:24-30.

418. Moreover, *Vardi* explains that “[i]f a ‘favorite’ **AP** (**AP** is called favorite if it is part of radio resource database that had been distributed to **client**...) is detected by the IEEE 802.11 scan ... the **client** can select this **AP** for connection, or If a list of previously successfully used **access points** is available (locally stored) and some **APs** on the list are available ... the client can select the **AP** ... for connection.” Ex. 1007, 13:13-23.

419. The asserted specifications also do not define “controlled by the server.” Ex. 1001. The only reference to “controlled by the server” in the specification of the 552 patent is to indicate that “the authenticated access point may include an access point controlled by mobile operating server.” Ex. 1007, 4:33-35.

420. *Vardi* discloses that the mobile device determines whether the **AP** is the preferred **AP**—an authenticated access point—by comparing the stored **API** (**APs** on the list under server control) with the **API** received from an *IEEE802.11* scan procedure.

421. “When [the] client becomes active it executes an IEEE 802.11 scan for **APs** in reach and determines the SSID, MAC address... Using the MAC address,

the client can compare this scan result with its radio resource database to determine which APs are preferred for connection...” Ex. 1007, 14:52-57.

422. That is, *Vardi* describes that the “radio resource database” is the stored access point information receive from the server. The mobile device compares the scan results, a POSITA understand the scan is a probe request and the results are a probe response, which includes the SSID and MAC address of the APs that responded. If an AP is not on the list, it is not under control of the server, however, if the AP is on the list it is under control of the server. Ex. 1001, cl. 24.

423. *Vardi* teaches or at least renders obvious that the APs are controlled by the server.

424. I have been asked to consider alternative positions PO may contend. One position PO may contend is that controlled by the server means that the server can engage in a request-response interaction with the AP.

425. In my opinion, if PO contends that a request-response interaction is the definition of controlled by the server, *Vardi* teaches that as well.

426. *Vardi* describes that the “[s]erver can also include an evaluation module, which can *evaluate[] accessibility, bandwidth and other characteristics of various AP[s]*, and store the information as an update in database...” Ex. 1007, 7:53-58. Subsequently, the server transmits this information to the mobile device.

427. *Vardi* further explains that the “server can include MappingType information that indicates the method by which the AP was mapped... where the server or the client *receives information about the location of an AP using two or more different methods of mapping*, location determination using one method can be selected to take precedence...” Ex. 1007, 16:47-54.

428. Under this definition, a POSITA would have readily understood *Vardi* disclosure to mean the server request “MappingType” information and the APs respond with the requested “MappingType” information.

429. I have been asked to consider PO’s infringement contention theory where PO alleges the probe request-response frames correspond to an AP “controlled by the server.”

430. *Vardi* teaches or at least renders obvious the same probe request-response communication depicted in PO’s infringement contention theory, including the SSID and MAC address. Ex. 1007, 10:25-36, 7:10-46, 9:54-64.

431. *Vardi* explains the mobile device can perform a “Basis **IEEE 802.11 association procedure**... using... **probing to get association information**” and “information acquired as part of the standard 802.11 scan, i.e.[,] Network or AP name (SSID—service set identifier); and, AP Radio Mac address” is included in the response from the AP. Additionally, under PO’s infringement theory, *Vardi* teaches or at least renders obvious that the APs are under control of the server because, the

“information” about the “relevant access points” is used by *Vardi*’s mobile device to perform a “Basic **IEEE 802.11 association procedure**... using **probing** to get association information” and “connect to the preferred access point.” Ex. 1007, 10:34-36, 3:4-7.

432. Because *Vardi*, like the ’552 patent, presumes a POSITA has working knowledge of IEEE 802.11, it does not provide the underlying details. However, a POSITA at the time of the alleged invention, would have readily understood that “IEEE 802.11 association procedure... using... probing” to mean the mobile device transmitting a probe request frame and the AP, in response, transmitting a probe response frame.

433. This is particularly true, here, where *Vardi* provides additional disclosures related to “IEEE scan” procedure and “IEEE association” procedure.

434. Ex. 1007, 10:25-28 (For example, “AP security status (e.g., WEP, WPA, WPAII)” “information can be tagged or association with information acquired as part of the standard 802.11 scan, i.e.: Network or AP name (SSID—service set identifier); and, AP Radio MAC address.”), 11:35-36 (“Select local usable wireless connections from IEEE 802.11 scan results.”), 12:17-20 (“when the AP is already part of radio resource database, only F1 (association), F2 (WPA exchange) and F4 are needed, thereby substantially reducing the average connection”), 13:4-7 (“Connecting to a wireless network starts by scanning the neighborhood for

candidate AP connections (IEEE 802.11 scan). The IEEE 802.11 scan can produce a list of access points in reach.”).

435. These additional disclosures inform a POSITA that *Vardi*’s “IEEE 802.11 scan” and “IEEE 802.11 association procedure” encompass IEEE 802.11 “Active Scan.” Thus, *Vardi* teaches or at least renders obvious PO’s infringement contention theory.

436. Even if PO contends that a POSITA would not have found *Vardi*’s disclosures of “probing,” “IEEE 802.11 scan” procedure, and “IEEE 802.11 association procedure” explicit, a POSITA would have naturally looked to *IEEE802.11* to supplement its understanding of *Vardi*’s “IEEE 802.11 scan” and “IEEE 802.11 association procedure” because *Vardi* directs a POSITA to *IEEE802.11*. See Section IX.F.1.

437. *IEEE802.11*’s disclosure is explicit. See *IEEE802.11*, Figure 4-17.

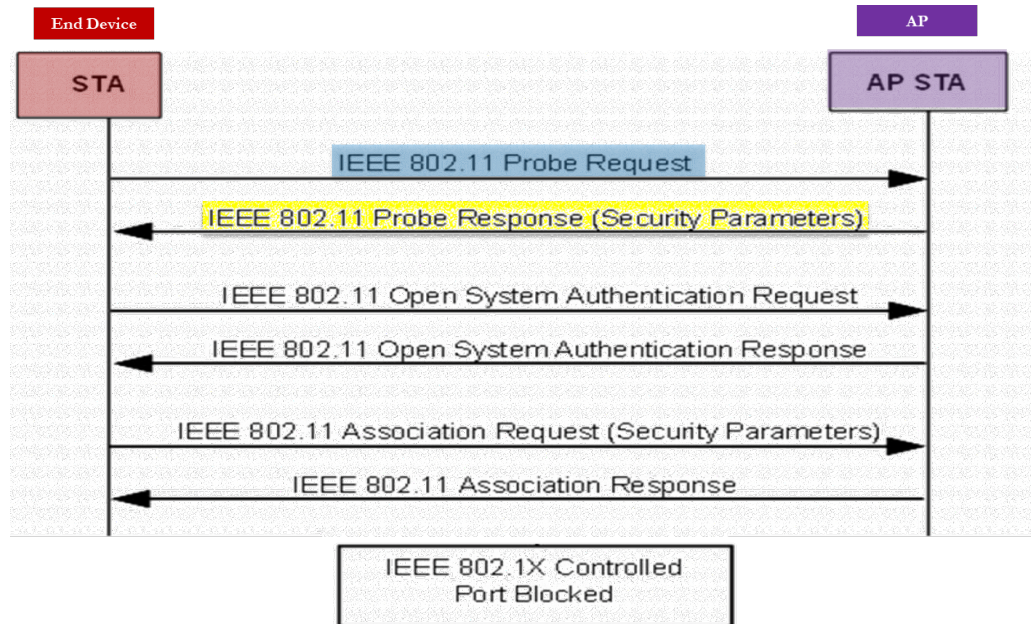


Figure 4-17—Establishing the IEEE 802.11 association

438. I have also considered whether the additional prior art references teach or render obvious APs “controlled by the server.”

439. In my opinion, *Orava* explains that the server assigns MAC address to the access points. Ex. 1005, ¶[54] (“In a server of the network, for example in the [] PAC, a list can be maintained to which the temporary MAC addresses allocated by the different access points AP are added. Thus, the AP can transmit a request for allocation of a temporary MAC address. On the basis of the request, the server selects an available address and transmits a response message comprising the allocated address MAC.”).

440. That is, address assignment demonstrates that the server controls the AP.

441. A POSITA would have found it obvious to combine the underlying implementation details of *IEEE802.11* and *Orava*'s server management capabilities to *Vardi*'s server. *See* Section IX.F.1.

442. First, both *Vardi* and *Orava* are built on top of *IEEE802.11* and thus, a POSITA would have known the standard aid in interoperable systems. *See* Section IX.F.1.

443. Second, a POSITA would have a likelihood of success as *Vardi* and *Orava* explicitly directs a POSITA to use *IEEE802.11*. Standards are meant to provide a reliable basis for people to share expectations, here, wireless connectivity. *See* Section IX.F.1.

444. Third, *Vardi* and *Orava* disclose a multi-AP system enabling connections between mobile devices, APs, and the Internet. A POSITA would have found it obvious to add *Orava*'s central server management capabilities, controlling the APs, to *Vardi*'s server because a POSITA would have understood the need to manage and distribute access point configurations within the system, for example, utilizing a single "SSID" for the "access points 370a-d." *See* Section IX.F.1.

445. A well-known example is moving through an office building, there a user's mobile device is connected to the SSID ("Office") despite as the user moves

floors connecting to a different access point. The APs are “controlled by the server,” where the server issues the same SSID for numerous APs. *IEEE802.11* (“4.3.13.12 Multiple BSSID capability – Multiple BSSID capability enables the advertisement of information for BSSIDs using a single Beacon or Probe Response frame instead of multiple Beacon and Probe Response frames, each corresponding to a single BSSID.”). *See* Section IX.F.1.

446. Moreover, *Orava*’s server management capabilities ensures that the randomly generated Fake IDs will be unique across APs by allocating specific MAC address space per AP. Ex. 1005, ¶[54] (“In a server of the network... a list can be maintained to which temporary MAC address allocated by the different [] AP are added... the server selects an available address and transmits a response...”). *See* Section IX.F.1.

447. In my opinion, a POSITA would have found it obvious to combine the teachings of *Vardi*, *IEEE802.11*, and *Orava* because their teachings align. *See* Section IX.F.1.

vii. Limitation 10[f]:

10[f]	transmitting, to the at least one access point in response to a
	determination that the at least one access point is the

authenticated access point, a connection request that includes an authentic device identifier for the device.

448. As explained in limitation 10[d], once the mobile device determines that the AP is the “preferred AP” (authenticated access point), the mobile device “selects for connection that AP.” *See* limitation 10[d] (§XI.A.1.v).

449. *Vardi* discloses that mobile devices store API received from the server in its memory, compare the stored API with the API received from an “IEEE 802.11 scan” to determine whether the AP is the preferred AP—the preferred AP being an authenticated access point—and automatically reconnect to that AP when the mobile device determines that the SSID or MAC address from the “IEEE 802.11 scan” matches that of the received authenticated access point list stored in memory. *See* limitations 10[a] (§XI.A.1.ii), 10[d]-[e] (§XI.A.1.v-§XI.A.1.vi).

450. Particularly, *Vardi* explains that “[w]hen client becomes active it executes an IEEE 802.11 scan for APs in reach and determines the SSID, MAC address... Using the MAC address, the client can compare this scan result with its radio resources database to determine which APs are preferred for connection...”). Ex. 1007, 14:52-57.

451. In other words, the mobile devices will compare the scan results with the database of access points previously connected to before issuing a connection

request to the AP. Indeed, *Vardi* describes “the connection process (F1 to F5) is being shortened as much as possible depending on whether radio resource information regarding the target AP is already known.” *Id.*, 13:36-39, 4-23.

452. I understand that PO’s infringement contentions draw a box around *IEEE802.11* “Authentication” and “Association” request-response frames for “a connection request that includes an authentic device identifier for the device.” Ex. 1011, 59-60.

453. *Vardi* teaches mobile devices establishing a connection to its preferred AP, for example, “‘favorite’ AP” to gain access to the Internet by performing “IEEE 802.11 association procedure” and comparing the scan results with the access point information received from the server to determine that the AP is the preferred AP. Ex. 1007, 13:13-17.

454. *Vardi* teaches or at least renders obvious transmitting a connection request to the preferred AP comprising an authentic device identifier, for example, the MAC address.

455. *Vardi* describes “[i]f a ‘favorite’ AP (AP is called favorite if it is part of radio resource database that had been distributed to client)... is detected by the IEEE 802.11 scan... the client can select this AP for connection...”

456. IEEE 802.11 is a term of art, which a POSITA would have readily understood corresponds to the “Active Scan” process, which includes the mobile

device transmitting a probe request and the AP transmitting, in response, a probe response.

457. Here, *Vardi*'s mobile device transmitted a probe request and "'favorite' AP" transmitted, in response, a probe response frame to the mobile device. *Vardi*'s mobile device compared its "radio resource database that had been distributed to [it]" from the server with the probe response and compared the "MAC address" to determine that "'favorite' AP" is its preferred AP and established connection.

458. *Vardi* presume a working knowledge of *IEEE802.11* and thus, do not provide the underlying implementation details a POSITA would readily understand at the time of the invention.

459. However, *Vardi* provides numerous disclosures to support that a POSITA would have found *Vardi* teaches or at least renders obvious issuing a connection request including the authentic device identifier.

460. *Vardi* explains that "[w]hen client becomes active it **executes an IEEE 802.11 scan** for APs in reach and determines the SSID, MAC address... Using the MAC address, the client can compare the scan result with the radio resource database to determine which **APs are preferred for connection** and roaming." *Id.*, 14:52-57.

461. *Vardi* explains that “[c]onnecting to a wireless network starts by scanning the neighborhood for candidate AP connections (IEEE 802.11 scan). The IEEE 802.11 scan can produce a list of access points in reach.” Ex. 1007, 13:4-7.

462. Further, *Vardi* teaches that the **mobile device** performs a “Basis IEEE 802.11 association procedure (inclusive of WEP, if needed); either using beacon information or *probing to get association information*” and the results of that scan comprise “Network or AP Name (SSID service set identifier); and, AP Radio MAC address.” Ex. 1007, 10:26-36.

463. *Vardi* also explains that “establishing a WiFi connection to the Internet requires a sequence of steps, starting with the IEEE 802.11 association...” Ex. 1007, 7:36-40.

464. A POSITA would have found each of these disclosures illustrative of a mobile device issuing a connection request as defined by *IEEE802.11*. Particularly, *Vardi*’s disclosure of a mobile device performing “Basic IEEE 802.11 association procedure (inclusive of WEP, if needed)” and “establishing a WiFi connection to the Internet requires a sequence of steps, starting with the IEEE 802.11 association...” See Section IX.F.1.

465. Because *Vardi* refers to IEEE 802.11 association procedure as “a sequence of steps” to “establish a WiFi connection to the Internet” a POSITA at the time of the alleged invention would have readily understood *Vardi* as teaching

the mobile device and AP proceed through each of the three steps until a connection to the Internet is established.

466. That is, *Vardi* teaches “probing” (issuing probe request/response frames), using “WEP” (authentication frame exchanges), and establishing WiFi connection to the Internet (association request/response frame exchanges).

467. Moreover, a POSITA knows that *Vardi*’s “IEEE 802.11 procedure must include three major steps as defined in *IEEE802.11*: (1) device discovery (“probing”); (2) device authentication (WEP, checking capabilities); and (3) establishing connection (association)” for the mobile device to “establish[] a connection to the Internet.” *See* Section IX.F.1.

468. Therefore, a POSITA would have readily understood at the time of the alleged invention that *Vardi* teaches or suggest a “connection request” and because *Vardi*’s disclosure is an “IEEE 802.11 association procedure,” a POSITA would have understood that the transmitted frames are defined by the standard and thus, the authentication and association frames include a MAC header, which comprises the MAC address of the mobile device. *See* Section IX.F.1.

469. The contents of a probe request/response, authentication request/response, and association request/response frame were well-known at the time of the alleged invention. The asserted patents themselves acknowledge this. Ex1001, 3:4-18 (describing the problem with IEEE use of MAC addresses “in order

to connect to a wireless local area network (WLAN), an end device may search for at least one available access point around the end device. By way of example, but not limitation, the access point may be a Wi-Fi access point and the WLAN may be a Wi-Fi network. When searching, the **end device may transmit a probe request frame that may include a device identifier, for the end device such as a media access control (MAC) address of the end device.** In such cases, **since the probe request frame that includes the device identifier is transmitted to access points around the end device,** present location information of the end device may be exposed to some access points with which a user of the end device does not want to be connected and/or other devices to which the end device does not want to disclose the present location information.”). *See IEEE802.11.*

470. Because *Vardi* presumes knowledge of IEEE 802.11 and explicitly directs a POSITA to its teachings, it is also my opinion, that a POSITA would have found it obvious to combine the underlying implementations details provided by *IEEE802.11* to *Vardi*’s communication system.

471. Particularly, *Vardi* directs a POSITA that the mobile device’s client performs IEEE authentication and association, that would naturally guide a POSITA to review the details of an IEEE authentication and association procedure to ensure compliance with the specification. *See* Section IX.F.1.

472. *IEEE802.11* defines that a “STA shall be able properly to construct a subset of the frames specified in this clause for transmission and to decode... All STAs shall be able to validate every received frame... and to interpret certain fields from the MAC headers of all frames.” *IEEE802.11*, 380.

473. It continues that “[e]ach frame consists of the following... *MAC header*... A variable-length *frame body*, which contains information specific to the frame *type* and *subtype*...” *IEEE802.11*, 380 (emphasis in original).

474. The general frame format transmitted includes a MAC Header followed by the frame body, which is depicted in Figures 8-1 and 8-2 (shown below).

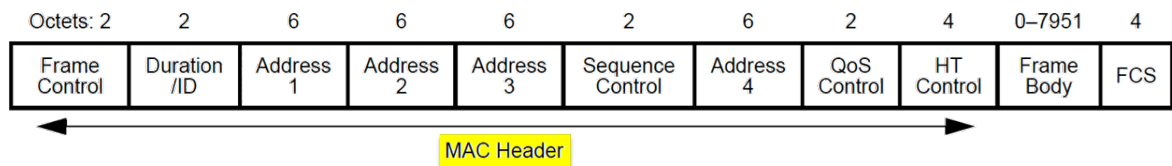


Figure 8-1—MAC frame format

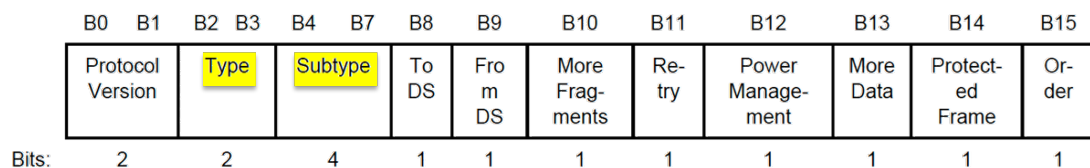


Figure 8-2—Frame Control field

475. Table 8-1 identifies valid type and subtype combinations. This is important because it identifies to a POSITA that “Association request,” “Association response,” “Authentication request,” and “Authentication response” are each of type “Management,” which dictates that it is transmitted with the MAC Header.

Table 8-1—Valid type and subtype combinations

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110	Timing Advertisement

Table 8-1—Valid type and subtype combinations (continued)

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication

476. Additionally, Figure 4-17 of *IEEE802.11* (shown below) corresponds to the same evidence cited to by PO in its infringement contention theory I was asked to consider.

477. The combination of this evidence supports my opinion that a POSITA would have found it obvious to combine *Vardi* with *IEEE802.11* to render obvious this limitation. *See* Section IX.F.1.

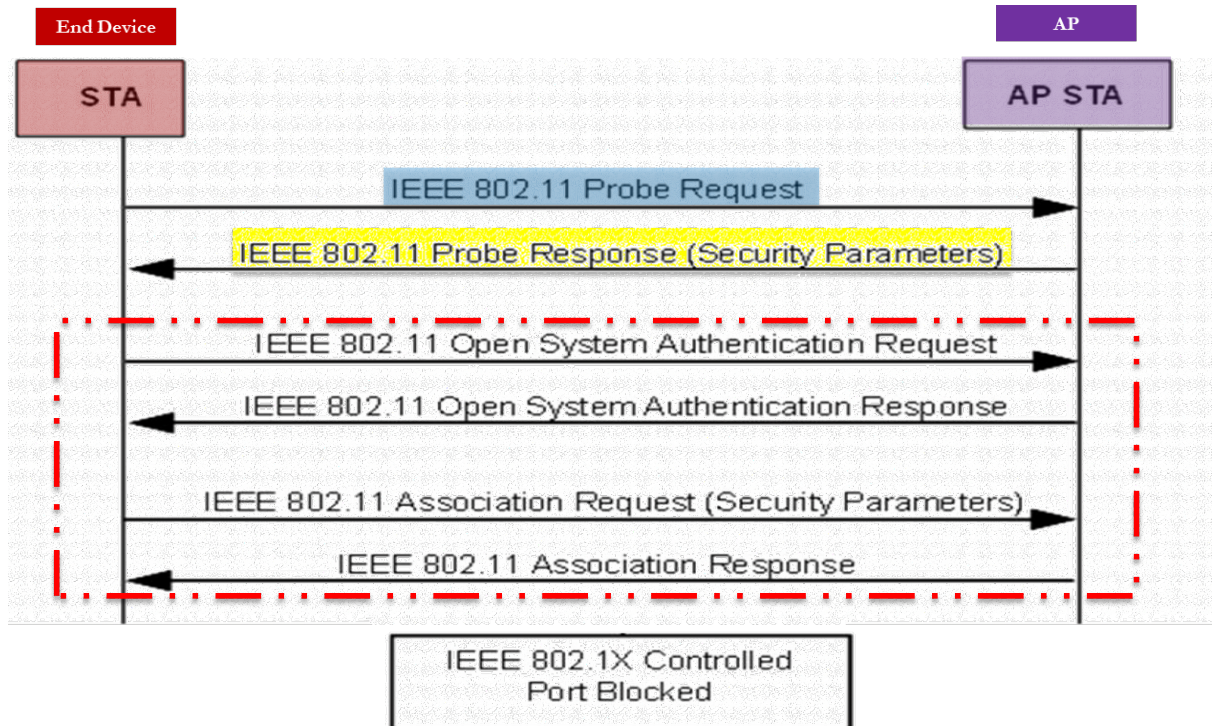


Figure 4-17—Establishing the IEEE 802.11 association

2. Claim 11

Claim 11 The method of claim 10, wherein the receiving the fake device identifier includes receiving a fake media access control (MAC) address.

478. In my opinion, *Vardi* in view of *IEEE802.11*, *Orava*, and *Yun* render obvious claim 11. *Orava* teaches “receiving the fake device identifier includes receiving a fake media access control (MAC) address.”

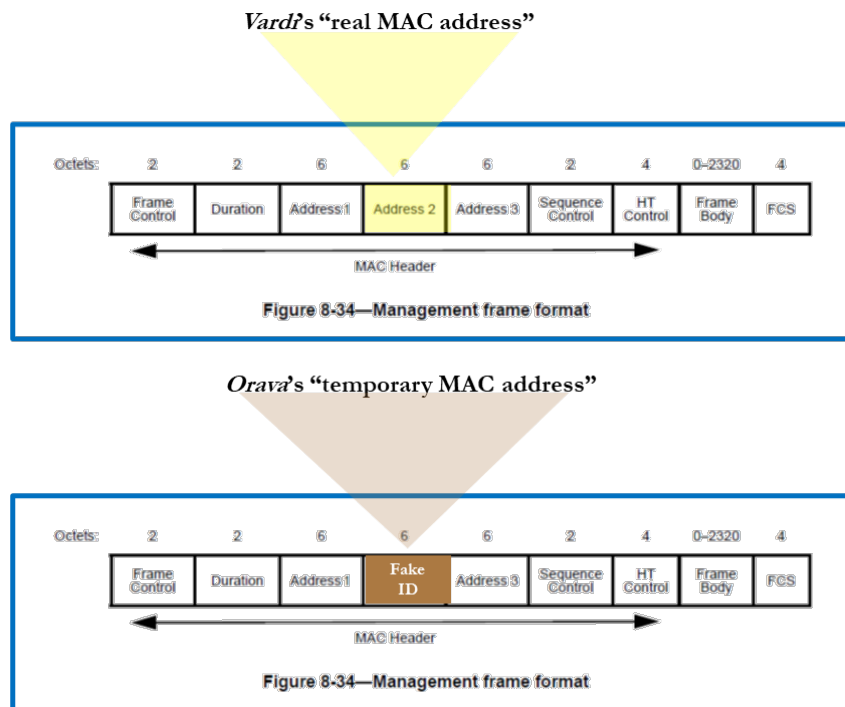
479. As I explain in more detail in limitation 10[b] (§XI.A.1.iii), *Orava* teaches transmitting a fake device identifier from a server to the mobile device. Ex. 1005, ¶[26] (“An MT transmits 203 a request comprising the identifier it has determined to a Second device to arrange a temporary MAC address. The second device may be a... a public access controller PAC... On the basis of the request, a temporary MAC address MAC can be arranged 205 in the second device to be used 204... The Second device transmits 205 a response frame relating to the arrangement of the MAC address comprising an identifier (MAC/REF)... the terminal MT can start using 207 the MAC address allocated to it.”).

480. As *Orava* explains, the fake device identifier can be generated in “IEEE 802 MAC address format...in which there are 46 available bits in a 48-bit address format for selecting the temporary MAC address.” Ex. 1005, ¶[30].

481. *Orava* explains that the “control of temporary MAC addresses may be centralized for instance in a public access controller PAC.” Ex. 1005, ¶[32].

482. For the reasons I explained above, a POSITA would have found it obvious to combine *Orava*’s fake device identifier with *Vardi*’s communication system. MAC address themselves are already randomly generated. And thus, swapping one random generated number for another, a POSITA would have had a high likelihood of success implementing. See Section IX.F.1.

483. Additionally, *Orava* instructs that it is “preferabl[e], the use of a temporary MAC address MAC does not, after the arrangement of the address, differ in any way from the use of a fixed MAC address permanently allocated by the manufacture,” and thus, a POSITA would have been motivated to maintain 802.11-compliance. Ex. 1005, ¶[49].



3. Claim 12

Claim 12	The method of claim 10, wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list comprises determining whether the at least one access point is under control of the server.
----------	--

484. In my opinion, *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 12. *See* limitation 10[a].

4. Claim 13

Claim 13	The method of claim 10, further comprising: storing the authenticated access point list in a memory.
----------	---

485. In my opinion, *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 13.

486. *Vardi* alone, in my opinion, teaches or at least renders obvious “storing the authenticated access point list in a memory.”

487. *Vardi* teaches that the mobile device receives API from the server and store it in its memory, which it later uses to compare with its scan results to determine whether the AP is the preferred AP. Ex. 1007, 7:23-32, 12:24-30, 13:13-23.

488. Storing previously connected APs was well-known in the art. An example, when a user comes home, the home owner’s mobile devices remembers its connection with the AP because it saved the access point information in memory.

489. *Vardi* also confirms that stating, “it is well known in prior art computing systems to cache information related to an access point to which the mobile device has connected before... the system uses this information in cache to automatically reconnect to that AP.” Ex. 1007, 12:24-30.

490. *Vardi* explains that “[t]he information gathered can provide access point connection or connectivity data that can be used by a wireless user terminal to connect to a specific access point... clients can store some or all of this information in the memory of the wireless user terminal.” Ex. 1007, 7:23-32.

491. *Vardi* also describes that the “connection process will exploit[ing] the radio resource information in its memory.” Ex. 1007, 13:4-23.

492. *Vardi* further explains connecting to “‘Favorite’ AP” by comparing scan results with the stored API received from the server. Specifically, *Vardi* explains, (“If a ‘favorite’ AP (AP is called favorite if it is part of radio resource database that had been distributed to client...) is detected by the IEEE 802.11 scan ... the client can select this AP for connection, or If a list of previously successfully used access points is available (locally stored) [in memory] and some APs on the list are available ... the client can select the AP ... for connection.” *Id.*

5. Claim 14

493. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 14.

- i. Limitation 14[pre]:
- ii. Limitation 14[a]:
- iii. Limitation 14[b]:
- iv. Limitation 14[c]:
- v. Limitation 14[d]:

14[pre]	The method of claim 10, further comprising:
14[a]	receiving, from the at least one access point, an approval of the connection request;
14[b]	transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;
14[c]	receiving, from the at least one access point, an association response to the association request; and
14[d]	connecting to a communication network via the at least one access point in accordance with the association response.

494. *Vardi* alone or in view of *IEEE802.11* renders obvious these limitations.

495. In my opinion, claim 14 only adds the steps outlined by *IEEE802.11* for connecting a mobile device to the Internet to claim 10.

496. *Vardi*, teaches or at least renders obvious this connection procedure, identified in *Vardi* as “IEEE 802.11 association.” Ex. 1007, 7:36-40, 10: 34-53 (“F1—Basic IEEE 802.11 association procedure (inclusive of WEP, if needed); either using beacon information or probing to get association information.”).

497. As I explain in the background section, there are three major 802.11 connection procedure steps: (1) device discovery (scanning); (2) device authentication (checking capability); and (3) establishment of connection (association). Corresponding to the three connection procedure steps, there are three corresponding connection states: (1) not authenticated or associated; (2) authenticated but not yet associated; and (3) authenticated and associated.

498. *Vardi* presumes knowledge of the 802.11 standard. Thus, a POSITA would have readily understood that *Vardi*'s disclosure referencing "IEEE 802.11 association" knows this disclosure corresponds to *IEEE802.11* Figure 4-17(below). And that "establishing a WiFi connection to the Internet requires a sequence of steps, starting with the IEEE 802.11 association, continuing with security exchange, essential network IP information acquisition and assessing specific network location." Ex. 1007, 7:36-43.

499. *Vardi* also describes these three states as "F1—Basic IEEE 802.11 association procedure (inclusive of WEP, if needed); either using beacon information or probing to get association information." Ex. 1007, 10:34-39. A mobile device must be authenticated and associated for data transfer (Internet connection).

500. In my opinion, a POSITA would have readily understood that to “establish[] a WiFi connection...starting with the IEEE 802.11 association” is inclusive of claim 14 as defined by *IEEE802.11*. See IX.F.1.

501. But even if I assume that a POSITA does not have this working knowledge, *Vardi* explicitly directs a POSITA to *IEEE802.11* for the underlying implementation of the “IEEE 802.11 association procedure.”

502. As shown below, *IEEE802.11* Figure 4-17 illustrates this procedure for an “Open System” authentication and association.

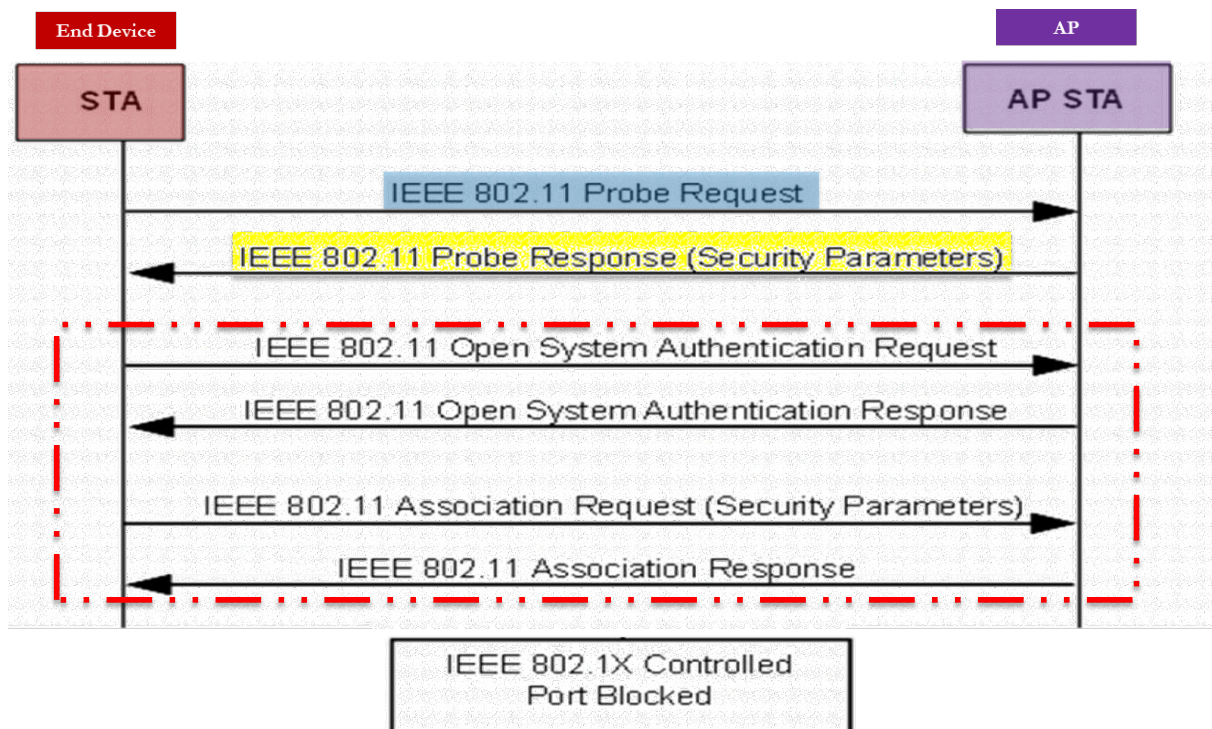


Figure 4-17—Establishing the IEEE 802.11 association

503. Thus, even if *Vardi* does not provide the underlying details of the connection procedure, which I believe it does to a POSITA, *Vardi* in view of *IEEE802.11* illustrates the connection procedure between the mobile device and AP in Figure 4-17 (shown above).

504. That is, *IEEE802.11* defines the connection procedure between a mobile device (“STA”) and an AP (“AP STA”). *IEEE802.11* illustrates that after the mobile device and AP exchange probe request and response frames, the mobile device transmits an authentication request, and the mobile device receives the AP’s transmitted authentication response, at which point the mobile device and AP are connected. Next, the mobile device transmits an association request frame, and the mobile device receives the AP’s transmitted association response frame, at which point the mobile device is authenticated and associated.

505. A POSITA would have naturally looked to *IEEE802.11* to provide the underlying implementation details of *Vardi*’s connection procedure and found it obvious to do so. *See* IX.F.1.

6. Independent Claim 15

506. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 15.

i. Limitation 15[pre]:

15[pre] A method performed by a device, the method comprising:

507. I understand that the preamble of claim 15 merely states the purpose or intended use of the claimed subject matter, which is not limiting.

ii. Limitation 15[a]:

15[a]	receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
-------	---

508. For the same reasons identified in claim 10, the combination renders obvious this limitation. *See*, limitation 10[a].

iii. Limitation 15[b]:

15[b]	generating a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;
-------	--

509. For the same reasons identified in claim 10, the combination renders obvious this limitation. *See*, limitation 10[b].

510. Limitation 15[b] appears to move the generation of the Fake ID from the server to the mobile device. *See* Ex. 1001, cl. 15 (“method performed by a device”).

511. Random generation capabilities were well-known at the time of the alleged invention and executing software to generate a random string was

conventional whether the software was executed on a server or the mobile device directly including in the context of randomizing MAC addresses.

512. A POSITA would not have found moving the random generation capability from one computing platform—the server—to another computing platform—the mobile device—to be a meaningful distinction.

513. Regardless of whether the Fake ID is generated at the server (claim 10) or on the mobile device (claim 15), *Orava* teaches or renders obvious this limitation.

514. *Orava* describes “[w]hen the terminal MT detects that the AP supports the use of temporary MAC addresses, *it determines* the MAC address MAC to be suggested.” Ex. 1005, ¶[29].

515. *Orava* explains that “MAC” is generated based upon a selection from one of the numerous algorithms including a random number generator, and the result is an IEEE MAC formatted address. Ex. 1005, ¶[30].

516. As I explained above, executing software was routine and a conventional procedure that mobile devices, at the time of the alleged invention, were expected to perform. Ex. 1007, 7:10-14 (“Each user's wireless user terminal can be a device that executes a program (e.g., a client) that uses the combined data to find usable radio resources or wireless APs and establish network connections through them, for example connections to the internet.”), cl. 8 (“A computer-readable medium including computer readable instructions that, when executed by

a computer, are configured to cause the computer to perform the following...”); Ex. 1005, ¶[21] (“Hardware solutions or a combination of hardware and software solutions may also be used to implement the inventive means.”). *See* IX.F.1.

517. In my opinion, it would have been obvious to a POSITA to add *Orava*’s random generation capabilities directly to the mobile device. Ex. 1005, ¶¶[4], [27].

518. *Orava* informs a POSITA of the “security risk” using the manufacturer generated MAC address and thus, a POSITA would have found it advantageous to maintain anonymity when connecting a user device to a WLAN by substituting the real MAC for a randomly generated MAC. Ex. 1005, ¶¶[4], [27].

519. *Vardi* and *Orava* disclose devices implementing IEEE 802.11-compliant MAC addresses.

520. A POSITA would have known that continuing to use the real MAC address exposed the user to location tracking and privacy concerns. Ex. 1005, ¶[3]. *See* IX.F.1.

521. It would have been obvious to a POSITA that maintaining interoperability is a high priority requirement, even while also allowing consumers to remain anonymous. *See* IX.F.1.

522. A POSITA would also have had a reasonable expectation of success in doing so because adding software to a mobile device was a conventional and

complying with the IEEE standard would have been typical and expected. *See* IX.F.1.

iv. Limitation 15[c]:

15[c]	transmitting, to at least one access point, a probe request frame that includes the fake device identifier;
-------	---

523. For the same reasons identified in claim 10, the combination renders obvious this limitation. *See*, limitation 10[c].

v. Limitation 15[d]:

15[d]	receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;
-------	--

524. For the same reasons identified in claim 10, the combination renders obvious this limitation. *See*, limitation 10[d] (§XI.A.1.v).

vi. Limitation 15[e]:

15[e]	determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether
-------	---

the at least one access point is the authenticated access point
includes determining whether the information regarding the at
least one access point is included in the authenticated access
point list that is received from the server, and wherein the
determining whether the information regarding the at least one
access point is included in the authenticated access point list
includes determining whether the at least one access point is
under control of the server; and

525. For the same reasons identified in claim 10, the combination renders obvious this limitation. *See*, limitation 10[e] (§XI.A.1.vi).

vii. Limitation 15[f]:

15[f]	transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.
-------	--

526. For the same reasons identified in claim 10, the combination renders obvious this limitation. *See*, limitation 10[f].

7. Claim 16

Claim 16	The method of claim 15, wherein the generating the fake device identifier includes generating a fake media access control (MAC) address.
----------	--

527. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 16.

528. *Orava*, in my opinion, teaches or at least renders obvious generating a fake identifier in “IEEE 802 MAC address format...in which there are 46 available bits in a 48-bit address format for selecting the temporary MAC address.” See limitation 10[b]; Ex. 1005, ¶¶[30][49].

529. A POSITA would have found it obvious to and been successful combining *Vardi* with *Orava*’s fake ID generation capabilities as described herein. See Section IX.F.1.

530. Particularly, *Orava* explains that “[p]referably, the use of a temporary MAC address MAC does not, after arrangement of the address, differ in any way from the use of a fixed MAC address permanently allocated by the manufacturer. The temporary MAC address can thus be used instead of a fixed address in all protocol messages.”

531. Additionally, MAC addresses themselves, are already randomly generated and thus, swapping one random address for another of the same format was a well-known and conventional.

8. Claim 17

Claim 17 The method of claim 15, wherein the information regarding the

at least one access point includes at least one of a media access

control (MAC) address of the at least one access point or a

service set identifier (SSID) of the at least one access point.

532. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 17.

533. *Vardi*, in my opinion, teaches or at least renders obvious the access point information including either the MAC or SSID.

534. In fact, *Vardi*'s access point information (API) includes both the SSID and MAC address. *See* limitation 10[b] (§XI.A.1.iii), 10[c] (§XI.A.1.iv), cl. 11 (§XI.A.2).

535. *Vardi* provides a listing of the API that the server transmits to the mobile device. The list includes both the "Network name," which corresponds to the SSID and the MAC address. Ex. 1007, 3:4-6, 25-29, 7:23-32.

536. *Vardi*'s "clients receive updates about relevant access points from the server and use the information to select and connect to the preferred access point." *Id.*, 3:4-6.

537. *Vardi* explains that the API "can include access point connectivity information that can be used by the wireless user terminal to connect to the access point." *Id.*, 3:25-29 (shown below).

i. Network name;
ii. MAC address;

iii. Received signal strength and variance over time;
iv. Encryption status;
v. Internet connection available capacity;
vi. Access protocol response times;
vii. Gateway IP address;
viii. DNS address;
ix. Occupied IP addresses;
x. Captive portal credentials;
xi. Connection Technology;

xii. User Terminal Location;
xiii. Access Point Location;
xiv. Mapping Type—how an access point location was determined.
The data base of data can comprise the above information as well as:
i. Location
ii. Internet accessibility
iii. Long term behavioral statistics comprising:
Percentage of availability
Signal strength variance
Available bandwidth
iv. Name of owner;
v. Owner profile;
vi. Password.

9. Claim 18

Claim 18	The method of claim 15, wherein the determining whether the at least one access point is the authenticated access point further includes determining whether the at least one access point was previously connected with the device.
----------	--

538. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 18. *See* limitation 10[e] (§XI.A.1.vi) and claim 12 (§XI.A.3).

539. *Vardi*, in my opinion, teaches or at least renders obvious “determining whether the at least one access point was previously connected with the device.”

540. As previously explained, *Vardi* teaches a mobile device compares scan results with API stored in its memory. The mobile device selects and connects to

that AP based on a previous connection, which *Vardi* terms a “preferred AP.” Ex. 1007, 13:4-23.

541. For example, *Vardi* details, “If a ‘favorite’ AP (AP is called favorite if it is part of radio resource database that had been distributed to client...) is detected by the IEEE 802.11 scan... (ex. Owner’s AP), the client can select this AP for connection or If a list of previously successfully used access points is available (locally stored) and some APs on the list are available... the client can select the AP... for connection.” *Id.*

542. Further, *Vardi* teaches, and I agree, that “it is well known in prior art computing systems to cache information related to an access point to which the mobile device has connected before... the system uses this information in cache to automatically reconnect to that AP.” Ex. 1007, 12:24-30.

10. Claim 19

Claim 19	The method of claim 15, further comprising: storing the authenticated access point list, received from the server, in a memory.
----------	---

543. In my opinion, *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 19.

544. *Vardi* alone, in my opinion, teaches or at least renders obvious “storing the authenticated access point list, received from the server, in a memory.”

545. *Vardi* teaches that the mobile devices receive API from the server and store it in memory, which it later uses to compare with its scan results to determine whether the AP is the preferred AP. Ex. 1007, 7:23-32, 12:24-30, 13:13-23.

546. I agree with *Vardi*’s disclosure that “it is well known in prior art computing systems to cache information related to an access point to which the mobile device has connected before... the system uses this information in cache to automatically reconnect to that AP.” *Id.*, 12:24-30.

547. *Vardi* explains that “[t]he information gathered can provide access point connection or connectivity data that can be used by a wireless user terminal to connect to a specific access point... clients can store some or all of this information in the memory of the wireless user terminal.” Ex. 1007, 7:23-32.

548. *Vardi* also describes that the “connection process will exploit[ing] the radio resource information in its memory.” *Id.*, 13:9-12.

549. *Vardi* further explains connecting to “‘Favorite’ AP” by comparing scan results with the stored API received from the server. Specifically, *Vardi* explains, (“If a ‘favorite’ AP (AP is called favorite if it is part of radio resource database that had been distributed to client...) is detected by the IEEE 802.11 scan ... the client can select this AP for connection, or If a list of previously successfully

used access points is available (locally stored) [in memory] and some APs on the list are available ... the client can select the AP ... for connection.” Ex. 1007, 13:13-23.

11. Claim 20

550. *Vardi, IEEE802.11*, and *Yun* render obvious Claim 20.

- i. Limitation 20[a]:
- ii. Limitation 20[b]:
- iii. Limitation 20[c]:
- iv. Limitation 20[d]:

Claim 20[a]	The method of claim 15, further comprising: receiving, from the at least one access point, an approval of the connection request;
-------------	---

Claim 20[b]	transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;
-------------	---

Claim 20[c]	receiving, from the at least one access point, an association response to the association request; and
-------------	--

Claim 20[d]	connecting to a communication network via the at least one access point in accordance with the association response.
-------------	--

551. *Vardi* alone or in view of *IEEE802.11* renders obvious the connection procedure outlined by claim 20.

552. In my opinion, claim 20 only adds the steps outlined by *IEEE802.11* for connecting a mobile device to the Internet.

553. *Vardi*, teaches or at least renders obvious this connection procedure, identified in *Vardi* as “IEEE 802.11 association.” Ex. 1007, 7:36-40, 10: 34-53 (“F1—Basic IEEE 802.11 association procedure (inclusive of WEP, if needed); either using beacon information or probing to get association information.”).

554. As I explain in the background section, there are three major 802.11 connection procedure steps: (1) device discovery (scanning); (2) device authentication (checking capability); and (3) establishment of connection (association). Corresponding to the three connection steps, there are three corresponding connection states: (1) not authenticated or associated; (2) authenticated but not yet associated; and (3) authenticated and associated.

555. *Vardi* presumes knowledge of the 802.11 standard. Thus, a POSITA would have readily understood that *Vardi*’s disclosure referencing “IEEE 802.11 association” knows this disclosure corresponds to *IEEE802.11* Figure 4-17 (above). And that “establishing a WiFi connection to the Internet requires a sequence of steps, starting with the IEEE 802.11 association, continuing with security exchange,

essential network IP information acquisition and assessing specific network location.” Ex. 1007, 7:36-43.

556. *Vardi* also describes these three states as “F1—Basic IEEE 802.11 association procedure (inclusive of WEP, if needed); either using beacon information or probing to get association information.” Ex. 1007, 10:34-39. A mobile device must be authenticated and associated for data transfer (Internet connection).

557. In my opinion, a POSITA would have readily understood that to “establish[] a WiFi connection...starting with the IEEE 802.11 association” is inclusive of claim 14 as defined by *IEEE802.11*.

558. But even if I assume that a POSITA does not have this working knowledge, *Vardi* explicitly directs a POSITA to *IEEE802.11* for the underlying implementation of the “IEEE 802.11 association procedure.”

559. As shown below, *IEEE802.11* Figure 4-17 illustrates this procedure for an “Open System” authentication and association.

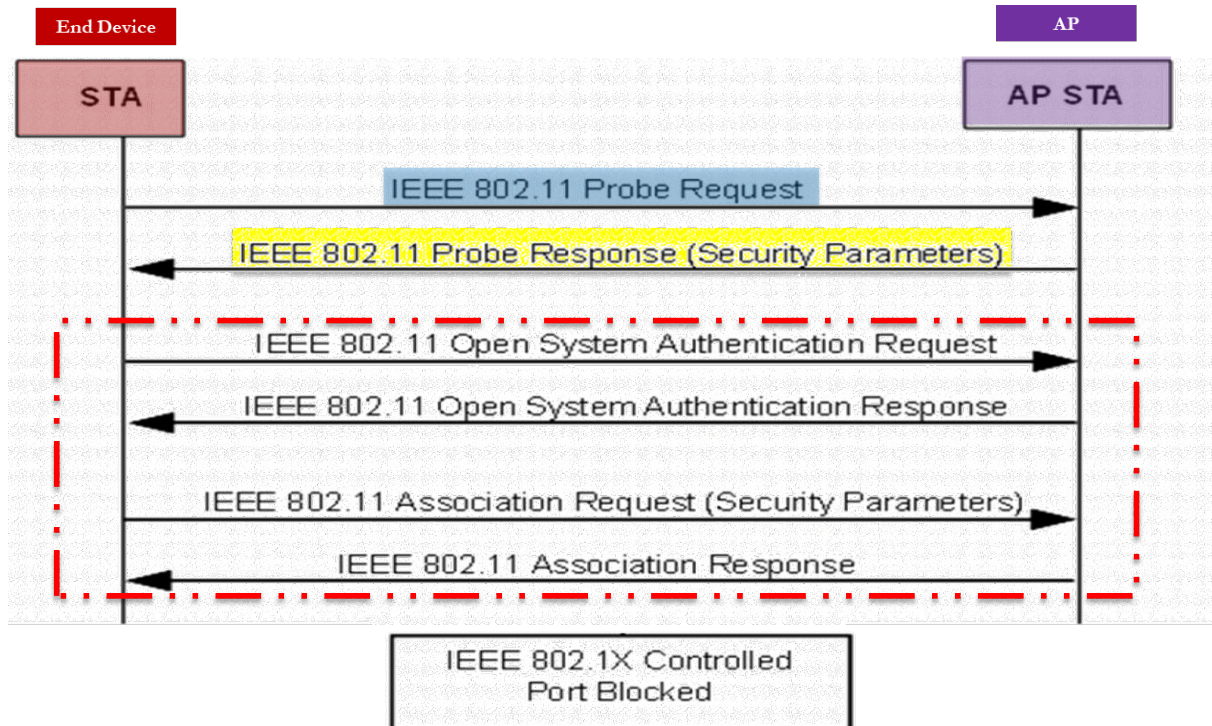


Figure 4-17—Establishing the IEEE 802.11 association

560. Thus, even if *Vardi* does not provide the underlying details of the connection procedure, which I believe it does to a POSITA, *Vardi* in view of *IEEE802.11* illustrates the connection procedure between the mobile device and AP in Figure 4-17 (shown above).

561. That is, *IEEE802.11* defines the connection procedure between a mobile device (“STA”) and an AP (“AP STA”). *IEEE802.11* illustrates that after the mobile device and AP exchange probe request and response frames, the mobile device transmits an authentication request, and the mobile device receives the AP’s

transmitted authentication response, at which point the mobile device and AP are connected. Next, the mobile device transmits an association request, and the mobile device receives the AP's transmitted association response, at which point the mobile device is authenticated and associated.

562. A POSITA would have naturally looked to *IEEE802.11* to provide the underlying implementation details of *Vardi*'s connection procedure and found it obvious to do so. *See* Section IX.F.1.

12. Independent Claim 21

563. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 21.

i. Limitation 21[pre]:

21[pre]	A method performed by a device, the method comprising:
---------	--

564. I understand that the preamble of claim 4 merely states the purpose or intended use of the claimed subject matter, which is not limiting.

565. For the same reasons identified in claim 10, the combination renders obvious this limitation. *See*, limitation 10[pre].

ii. Limitation 21[a]:

21[a]	receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
-------	---

566. For the same reasons identified in claim 10, the combination renders obvious this limitation. *See*, limitation 10[a] (§XI.A.1.ii).

iii. Limitation 21[b]:

21[b]	generating a collection that includes at least one of one or more random numbers or one or more random characters to provide a fake device identifier for the device to falsely identify the device in a probe request frame;
-------	---

567. For the same reasons identified in claim 10, the combination renders obvious this limitation. *See*, limitations 10[b] (§XI.A.1.iii).

iv. Limitation 21[c]:

21[c]	transmitting, in a search for at least one available access point around the device, the probe request frame that includes the fake device identifier;
-------	--

568. For the same reasons identified in claim 10, the combination renders obvious this limitation. *See*, limitation 10[c] (§XI.A.1.iv).

v. Limitation 21[d]:

21[d]	receiving, from at least one access point around the device in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;
-------	--

569. For the same reasons identified in claim 10, the combination renders obvious this limitation. *See*, limitation 10[d] (§XI.A.1.v).

vi. Limitation 21[e]:

21[e]	determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list, and wherein the determining whether the information regarding the at least one access point is included in the
-------	---

authenticated access point list includes determining whether the
at least one access point is under control of the server; and

570. For the same reasons identified in claim 10, the combination renders obvious this limitation. *See*, limitation 10[e] (§XI.A.1.vi).

vii. Limitation 21[f]:

21[f]	transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.
-------	--

571. For the same reasons identified in claim 10, the combination renders obvious this limitation. *See*, limitation 10[f] (§XI.A.1.vii).

13. Claim 22

Claim 22	The method of claim 21, wherein: the generating the collection that includes the at least one of one or more random numbers or one or more random characters comprises configuring the collection as a fake media access control (MAC) address, and the
----------	--

fake device identifier includes the fake media access control
(MAC) address.

572. As explained in claim 15, *Orava* teaches or at least renders obvious an on-device generation of the Fake ID. See claim 15; Ex. 1005, ¶[29].

573. When the terminal MT detects that the AP supports the use of temporary MAC addresses, it determines the MAC address MAC to be suggested. *Id.*, ¶[29].

574. *Orava* describes that the fake ID is generated upon a selection from one of the numerous algorithms including a random number generator, and the result is an IEEE MAC formatted address. Ex. 1005, ¶[30].

575. MAC can be a random number generated by means of a random number generator. MAC can be selected from the address space allocated to the MT on the basis of an address selection algorithm. A temporary MAC address MAC can be allocated to the MT for instance from among organization-specific unique identifiers (OUI) reserved for this purpose. Typically, one OUI allows $2^{\{ \text{circumflex over } () \} 24}$ addresses. The IEEE 802 MAC address format allows locally administrable MAC addresses, in which there are 46 available bits in a 48-bit address format for selecting the temporary MAC address. A MAC address can also be formed of a

network identifier, such as a BSS identifier BSSID, and of a random part added thereto, for example. *Id.*

576. A POSITA would have found it obvious to and been successful combining *Vardi* with *Orava*'s fake ID generation capabilities as described herein. *See* Section IX.F.1.

577. *Orava* explicitly instructs a POSITA that "MAC" follows the IEEE MAC address format, *IEEE802.11* "allows locally administrable MAC addresses," and that "[p]referably, the use of a temporary MAC address MAC does not, after arrangement of the address, differ in any way from the use of a fixed MAC address permanently allocated by the manufacturer. The temporary MAC address can thus be used instead of a fixed address in all protocol messages." Ex. 1005, ¶¶[30], [49]

578. Additionally, MAC addresses themselves, are already randomly generated and thus, swapping one random address for another of the same format was a well-known and conventional. *See* Section IX.F.1.

14. Claim 23

23	The method of claim 21, further comprising: storing the fake device identifier in a memory.
----	---

579. In my opinion, *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 23.

580. In my opinion, *Orava* teaches or at least renders obvious storing the fake ID in memory.

581. *Orava* explains, “Each MAC address determines a temporary or fixed context.” *Id.*, ¶[70].

582. *Orava* also teaches “the terminal MT must request for reconfirmation of the temporary MAC address MAC (indicate in request 304, 405 that it is not new MAC address) if the address has not been used for a long time.” *Id.*, ¶[58].

583. A POSITA would have readily understood *Orava*’s specification is describing using and re-using the randomly generated MAC address and thus, it is stored in memory. *See* Section IX.F.1.

15. Independent Claim 24

- i. Limitation 24[pre]:
- ii. Limitation 24[a]:
- iii. Limitation 24[b]:
- iv. Limitation 24[c]:
- v. Limitation 24[d]:
- vi. Limitation 24[d.i]:
- vii. Limitation 24[d.ii]:

24[pre]	A system, comprising:
---------	-----------------------

24[a]	a processor;
-------	--------------

24[b]	at least one communication interface;
24[c]	a transmitter to transmit, to at least one access point via the at least one communication interface, a probe request frame that includes a fake device identifier for a device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;
24[d]	a receiver to:
24[d.i]	receive, from the at least one access point via the at least one communication interface, a probe response frame that includes information regarding the at least one access point; and
24[d.ii]	receive, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;

584. *Vardi, IEEE802.11, Orava and Yun* render obvious limitations 24[pre]-24[d.ii]. *See* Limitations 10[a]-[d] (§XI.A.1.ii-§XI.A.1.v).

585. **Processor.** Specifically, *Vardi* describes a “processor” executes a client program for finding usable APs and establishing network connections through them.

586. *Vardi* further explains that the system can employ a client/server architecture where the client is a software program executed on the device. Ex. 1007, 7:10-20. Claim 8 preamble recites, “computer readable medium including computer readable instructions that, when executed by a computer, are configured to cause the computer to perform the following...”

587. *Vardi*, in my opinion, explicitly discloses a “processor” because it discloses a system executing software on a mobile device. Further, at the time of the alleged invention, it was well-known, routine, and conventional for mobile devices to include a “processor.”

588. But I was also asked to consider whether any other reference also disclosed the use of a “processor” in the prior art. *Orava* does. *Orava* ¶[21].

589. *Orava* discloses “MT comprises... a central processing unit CPU comprising one or more processors.” Ex. 1005, ¶[21].

590. **Communication Interface (transmitter/receiver).** As I explained above, *Vardi* describes mobile devices connecting to the Internet wirelessly. A POSITA would have found *Vardi*’s disclosure explicit.

591. Specifically, *Vardi* teaches “clients continuously collect radio resource information about APs detected by the wireless user terminal... clients can be executed on laptops, handheld devices (PDA’s), cellphones, or any other devices that incorporates a radio facility for wireless communication, such as WiFi.” Ex. 1007, 9:54-62.

592. FIG. 3 (depicting mobile devices in wireless communication with a server and APs), 14:66-15:1 (“In FIG. 3 In FIG. 3, a computing resource, such as server 310, and radio access points 370 a-d are connected to a network 305, such as the Internet “).

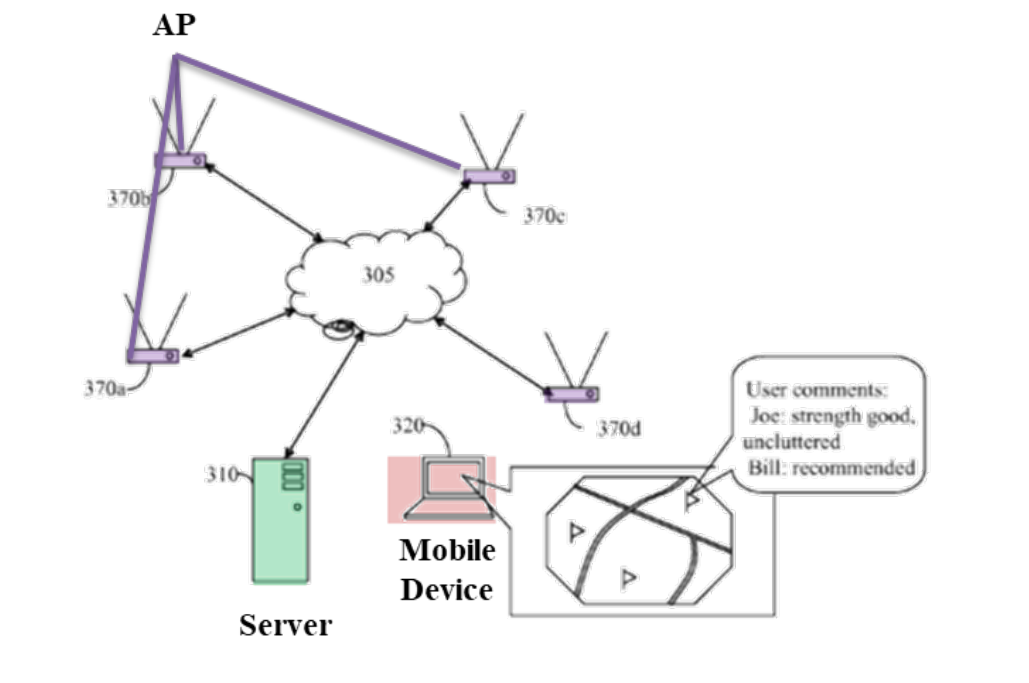


Figure 3

593. *Vardi* further explains that each of these mobile devices incorporate “a radio facility for wireless communication,” which a POSITA would have readily understood to correspond to the claimed “communication interface” and that “communication interface” comprises a “transmitter” and a “receiver” to, as *Vardi* explains, “Clients receive updates about relevant access points from the server and use the information to connect to the preferred access point. The clients also check connectivity to other access points in the vicinity, and report the findings to the server.” These operations are well-known and directly correspond to a mobile device that comprises “a transmitter to transmit” and “a receiver to receive.” Ex. 1007, Abstract, 3:11-13 (“connecting a wireless user terminal to a network, such as the internet,”), 3:62-63 (the device “transmitting the first set of data to a server over a network or the Internet,”), 5:12-15, 9:54-62, 14:52-57 (“When client becomes active it executes an IEEE 802.11 scan for APs in reach and determines the SSID, MAC address...”), 17:61-63.

594. However, I have also considered other prior art references should the patent owner contend otherwise and *Orava* is also explicit in its disclosure of these well-known components.

595. Ex. 1005, ¶¶[21] (“MT comprises at least memory, a transceiver for arranging wireless communications, and [1] a central processing unit CPU comprising one or more processors.”), [30] (“random number generator”).

596. A “transceiver” is a device that can both transmit and receive signals.
Ex. 1008, 3 (“Transceiver: A device that can both transmit and receive signals.”).

597. For the reasons explained herein, a POSITA would have found it obvious to combine these well-known components with *Vardi*’s mobile device as these components are being used in their ordinary course of operation in compliance supporting the IEEE 802.11 standard. *See* Section IX.F.1.

viii. Limitation 24[e]:

24[e]	a memory to store the information regarding the at least one access point, and the authenticated access point list; and
-------	--

598. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious limitation 24[e].
See Limitation 10[d] (§XI.A.1.v), cl. 13 (§XI.A.4).

599. *Vardi* explains that “(“user’s clients can store some or all of this information in the memory of the wireless user terminal to a... wireless access point to connect to.”

600. Additionally, *Orava* discloses “MT comprises at least memory.” Ex. 1005, ¶[21].

ix. Limitation 24[f]

x. Limitation 24[g]

24[f] a determination unit to determine, under control of the processor and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point and is under control of the server,

24[g] wherein to determine whether the at least one access point is the authenticated access point and is under control of the server, the determination unit determines whether the information regarding the at least one access point is included in the authenticated access point list, and

601. *Vardi*, *IEEE802.11*, *Orava* and *Yun* render obvious limitations 24[f]–[g]. *See* limitations 10[a](§XI.A.1.ii), 10[d] – 10[e] (§XI.A.1.v–§XI.A.1.vi).

602. Limitations 24[f] and [g] add “a determination unit to determine” the same method steps of claim 10.

603. *Vardi* discloses the “determination unit.” Ex. 1007, 7:10-20, 13:13-23, 14:52-57.

604. Specifically, *Vardi* explains “wireless user terminal can be a device that executes a program (e.g., a client)... The client can be a software program executed on the wireless user terminal,” which is the “determination unit ... under control of the processor.” Ex. 1007, 7:10-20.

605. *Vardi* further explains that “[w]hen client becomes active it executes an IEEE 802.11 scan for APs in reach and determines the SSID, MAC address... Using the MAC address, the client **can compare this scan result with its radio resources database to determine which APs are preferred for connection** and roaming.”
Id., 14:52-57.

606. As I explained above, *Vardi* teaches or at minimum renders obvious the “processor,” however, it would have also been obvious to implement *Orava*’s processor as part of *Vardi*’s mobile device to execute the client software performing the determination whether the AP is the preferred AP.

xi. Limitation 24[h]

Claim 24[h]	wherein the transmitter further transmits to the at least one access point, a connection request that includes an authentic device identifier for the device, in response to a determination by the determination unit that the at least one access point is the authenticated access point and is under control of the server.
-------------	---

607. *Vardi*, *IEEE802.11*, *Orava* and *Yun* render obvious limitations 24[f]–[h].

608. Again, limitation 24[h] differs only that it adds a “transmitter” to the method performed in claim 10. *See* Ex. 1001, cl. 10, 24. Transmitters are well-

known components of mobile devices as I explained above for “communication interface.” *See* limitations 24[b] – [c] (§XI.A.1.iii-§XI.A.1.iv).

609. Explained there, *Vardi-IEEE802.11-Orava-Yun*’s mobile device transmits a connection request to the determined preferred AP.

16. Claim 25

Claim 25	The system of claim 24, wherein the fake device identifier includes a fake media access control (MAC) address.
----------	--

610. *Vardi, IEEE802.11, Orava*, and *Yun* render this claim obvious.

611. In my opinion, *Orava* teaches or at least renders obvious the fake ID includes a MAC address, because as I explained in limitation 10[b] (§XI.A.1.iii) and 11 (§XI.A.2), *Orava* teaches that the fake identifier is in “IEEE 802 MAC address format...in which there are 46 available bits in a 48-bit address format for selecting the temporary MAC address.” Ex. 1005, ¶[30].

612. For the reasons I explained above, a POSITA would have found it obvious to combine *Orava*’s fake device identifier with *Vardi*’s communication system. MAC address themselves are already randomly generated. And thus, swapping one random generated number for another, a POSITA would have had a high likelihood of success implementing.

613. Additionally, *Orava* instructs that it is “preferabl[e], the use of a temporary MAC address MAC does not, after the arrangement of the address, differ in any way from the use of a fixed MAC address permanently allocated by the manufacture,” and thus, a POSITA would have been motivated to maintain 802.11-compliance. Ex. 1005, ¶[49].

17. Claim 26

Claim 26	The system of claim 24, further comprising: a fake device identifier generation unit to generate, under control of the processor, the fake device identifier.
----------	---

614. *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render this claim obvious.

615. Claim 26 differs from claim 10 and 11 in that it adds “generation unit to generate, under the control of the processor.” *Orava* teaches or renders this addition obvious as well. Ex. 1005, ¶¶[21], [30]; Ex. 1007, Figure 3 (annotated below).

616. Both *Vardi* and *Orava* teach the mobile device comprises a processor. Ex. 1007, 7:10-20 (“wireless user terminal can be a device that executes a program (e.g., a client)... The client can be a software program executed on the wireless user terminal,” the claimed “determination unit... under control of the processor.”); Ex. 1005, ¶[21] (“CPU comprising one or more processors”).

617. *Orava* teaches that the “processor” executes computer code for generating random MAC addresses. *Id.* (“Computer program codes executed in the [] CPU can cause the terminal MT to implement inventive means, some embodiments of which are illustrated in FIGS. [2-7]. Hardware solutions or a combination of hardware and software solutions may also be used to implement the inventive means.”)

618. A POSITA would have found it obvious, for the reasons explained herein, to combine *Orava*’s on-device random generator capabilities to *Vardi*’s mobile device. The combination requires nothing more than adding the software to *Vardi*’s mobile device, which is routine and conventional task for a POSITA.

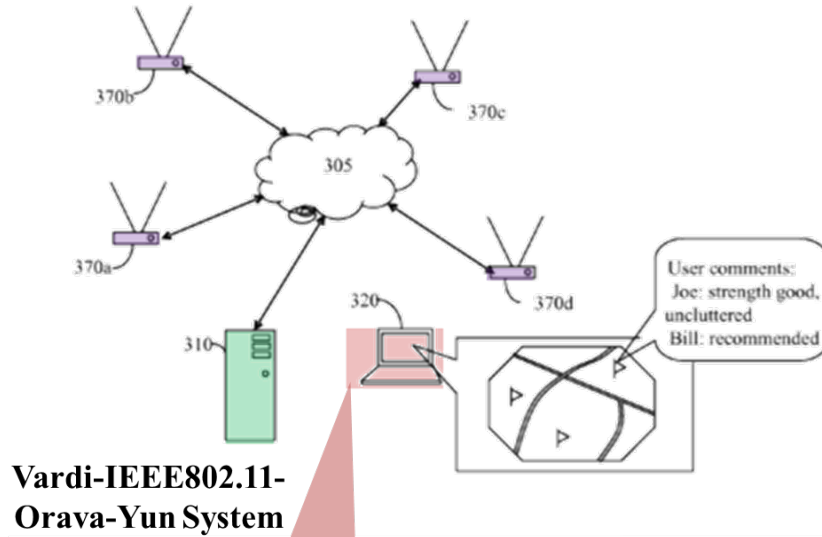
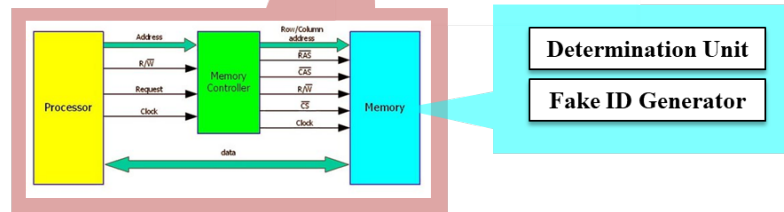


Figure 3



18. Claim 27

27 The system of claim 24, wherein the memory further stores the fake device identifier.

619. In my opinion, *Vardi*, *IEEE802.11*, *Orava*, *Yun* and *Kholaif* render obvious claim 27. *See* limitations 10[b] (§XI.A.1.iii) and claim 23 (§XI.A.14).

620. In my opinion, *Orava* teaches or at least renders obvious storing the Fake ID in memory.

621. *Orava* explains, “Each MAC address determines a temporary or fixed context.” Ex. 1005, ¶[70].

622. *Orava* also teaches “the terminal MT must request for reconfirmation of the temporary MAC address MAC (indicate in request 304, 405 that it is not new MAC address) if the address has not been used for a long time.” *Id.*, ¶[58].

623. A POSITA would have readily understood or found it obvious that *Orava*’s specification is describing using and re-using the randomly generated MAC address and thus, it is stored in memory. A POSITA would want to save the Fake ID so that it does not have to continuously re-generate the Fake ID and thus, could not guarantee the same Fake ID for its next use.

624. For the reasons explained in Section IX.F.1 it would have been obvious to combine *Orava*’s random generation capabilities with *Vardi*’s mobile device.

19. Claim 28

Claim 28	The system of claim 24, wherein the at least one access point includes a Wi-Fi access point, and wherein the at least one communication interface is configured for communication with a Wi-Fi network.
----------	---

625. In my opinion, *Vardi*, *IEEE802.11*, *Orava*, and *Yun* render obvious claim 27.

626. In my opinion, *Vardi* teaches or at least renders obvious the AP including a Wi-Fi access point and the mobile device's communication interface is configured to communication with the Wi-Fi network. Ex. 1007, 14:66-15:1, 7:6-43, 9:54-59, 5:11-16, 7:36-40, Figure 3.

627. In my opinion, a POSITA would have readily understood that *Vardi*'s mobile devices teach or at least render obvious a communication interface as I explained in claim 24 that communicate with APs that include WiFi capabilities.

628. *Vardi* explains that “[i]n FIG. 3, a computing resource, such as server 310 and radio access points 370a-d are connected to a network 305, such as the Internet.” Ex. 1007, 14:66-15:1; *see* Section IX.F.1.

629. *Vardi* explains clients continuously collect radio resources information about APs detected by the wireless user terminal. These clients can be executed on laptops, handheld devices (PDA's), cellphones, or any other devices that incorporates a radio facility for wireless communication, such as WiFi.” *Id.*, 9:54-59.

630. *Vardi* discloses “Wifi enabled mobile telephones.” *Id.*, 5:11-16.

631. *Vardi* teaches “the invention, methods and systems are described that evaluate historical data discovered by the user community (such as WiFi ‘hot-spots’ locations and quality)...” *Id.*, 7:6-10.

632. Additionally, *Vardi* teaches that the “radio resource database 150 stores data on all radio access points (WiFi and others) that have been discovered or registered by the user community.” *Id.*, 11:27-30.

XII. IPR2024-01369 GROUND 2: *VARDI*, *IEEE802.11*, *ORAVA* AND *YUN* RENDER CLAIMS 24-28 OBVIOUS

A. Obviousness of Claims 24-28

633. In my opinion *Vardi*, *IEEE802.11*, *Orava*, *Yun*, and *Kholaiif* render obvious claims 24-28.

634. In my opinion, *Vardi* alone or in view of *Orava* teaches or renders obvious the hardware components claimed in claim 24 as I explained above. *See* Section XI.A.15.

635. I have also considered whether any additional prior art disclosed the well-known components if PO contends otherwise. *Kholaiif* explicitly discloses each of the claimed components and a POSITA would have found it obvious to combine with *Vardi*, *IEEE802.11*, *Orava*, and *Yun*.

636. At the time of the alleged invention, each of the claimed components were well-known and the claims use those components in their conventional manner.

637. I incorporate my analysis above and focus specifically on the hardware components. *See* Section XI.A.15.

1. Independent Claim 24

638. *Vardi*, *IEEE802.11*, *Orava*, *Yun*, and *Kholaiif* render obvious Claim 24.

639. Claim 24 recites a system comprising, in my opinion, well-known mobile device components to perform the same method identified in claim 10.

640. For the same reasons identified in claim 10, the combination renders obvious claim 24. *See* claim 10.

641. A POSITA reading *Vardi* would have found each of these components taught or at minimum obvious. Ex. 1007, Title (“System and Method for Mapping Wireless Access Points”), Abstract (“Clients **receive** updates about relevant access points **from the server** and **use the information to connect to the preferred access point**. The **clients also check connectivity** to other access points in the vicinity, and **report the findings to the server**. The server uses the reports to update its database, and send corresponding updates to the clients. The database can include information about the location of the access points. The information about the location of the access points can be manually input or determined using GPS information.”), FIG. 3, 14:66-15:1 (“In FIG. 3 In FIG. 3, a computing resource, such as server 310, and radio access points 370 a-d are connected to a network 305, such as the Internet “).

642. Each of these well-known mobile device components are disclosed by *Vardi* and a POSITA would have found *Vardi*’s disclosure explicit.

- i. Limitation 24[pre]:
- ii. Limitation 24[a]:

- iii. Limitation 24[b]:
- iv. Limitation 24[c]:
- v. Limitation 24[d]:
- vi. Limitation 24[d.i]:
- vii. Limitation 24[d.ii]:
- viii. Limitation 24[e]:

24[pre]	A system, comprising:
24[a]	a processor;
24[b]	at least one communication interface;
24[c]	a transmitter to transmit, to at least one access point via the at least one communication interface, a probe request frame that includes a fake device identifier for a device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;
24[d]	a receiver to:
24[d.i]	receive, from the at least one access point via the at least one communication interface, a probe response frame that includes information regarding the at least one access point; and

24[d.ii] receive, from a server, an authenticated access point list that

 includes information regarding one or more access points that are

 controlled by the server;

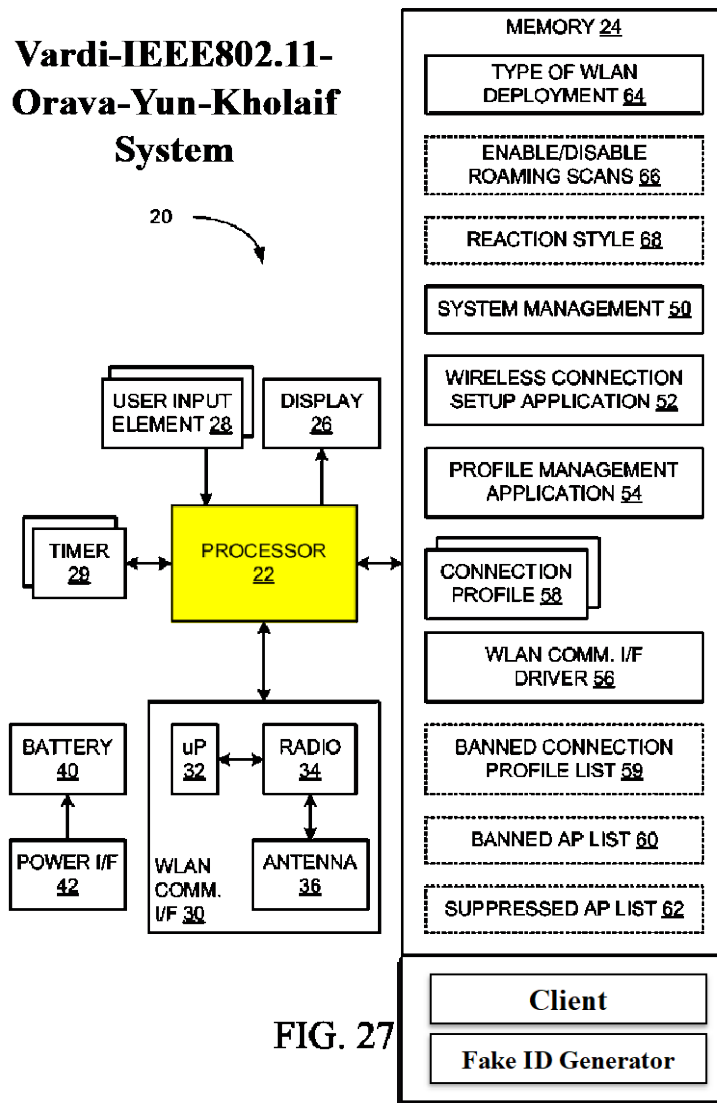
24[e] a memory to store the information regarding the at least one

 access point, and the authenticated access point list; and

643. A POSITA would have readily known at the time of the alleged invention, that mobile devices comprise these well-known components: (1) processor; (2) communication interface; (3) transmitter; (4) receiver, and (5) memory.

644. Kholaiif discloses “FIG. 27 is a functional block diagram illustration of an example mobile station, which can be considered an example of any one of **mobile stations** 106, 116 and 136. The example **mobile station**, generally referenced 20, comprises a **processor** 22, a **memory** 24, a display 26, one or more user input elements 28, one or more timers 29, and a **WLAN communication interface** 30. A non-exhaustive list of examples for user input elements 28 includes a keypad, a keyboard, a trackball, and a thumbwheel. Some mobile stations use a touchscreen, which functions both as display 26 and as one of the user input elements 28. **WLAN communication interface** 30 comprises a **baseband processor** 32

coupled to a radio 34, which in turn is coupled to an antenna 36.” Ex. 1010, ¶[242], Figure 27.



645. A POSITA would have looked to and for components that support IEEE 802.11 standard communications when deploying mobile devices in a *IEEE802.11* WLAN and would have found success implementing them because that is one of the main purposes of a standard, ensuring compliance and compatibility. *See*

ix. Limitation 24[f]:

x. Limitation 24[g]:

24[f]	a determination unit to determine, under control of the processor and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point and is under control of the server,
-------	---

24[g]	wherein to determine whether the at least one access point is the authenticated access point and is under control of the server, the determination unit determines whether the information regarding the at least one access point is included in the authenticated access point list, and
-------	--

646. Limitations 24[f] and [g] add a “determination unit to determine” the steps addressed in claim 10.

647. *Kholaiif* teaches “mobile station... comprises a processor.” *Id.*, ¶[242], Figure 27.

648. It would have been obvious to a POSITA at the time of the alleged invention to implement *Kholaiif*’s processor as part of *Vardi*’s mobile device to execute the client software performing the determination whether the AP is the preferred AP. *See* claim 24 (§IX.F.1).

xi. Limitation 24[h]

Claim 24[h] wherein the transmitter further transmits to the at least one access point, a connection request that includes an authentic device identifier for the device, in response to a determination by the determination unit that the at least one access point is the authenticated access point and is under control of the server.

649. As I explained for limitation 24[c], *Kholaiif* teaches a “transmitter.” *See* limitation 24[c].

2. Claim 25

Claim 25 The system of claim 24, wherein the fake device identifier includes a fake media access control (MAC) address.

650. As I explained for limitation 24[c], *Kholaiif* teaches a “transmitter.” *See* limitation 24[c]. *See* cl. 25 (§XI.A.16).

3. Claim 26

Claim 26 The system of claim 24, further comprising: a fake device identifier generation unit to generate, under control of the processor, the fake device identifier.

651. In my opinion, *Vardi*, *IEEE802.11*, *Orava*, *Yun*, and *Kholaiif* render obvious claim 26. See cl. 26 (§XI.A.17).

4. Claim 27

27	The system of claim 24, wherein the memory further stores the fake device identifier.
----	---

652. In my opinion, *Vardi*, *IEEE802.11*, *Orava*, *Yun*, and *Kholaiif* render obvious claim 27. See cl. 27 (§XI.A.18).

653. *Kholaiif* teaches “mobile station... comprises... a memory.” *Id.*, ¶[242], Figure 27.

654. It would have been obvious to a POSITA at the time of the alleged invention to implement *Kholaiif*’s memory as part of *Vardi*’s mobile device to store the fake ID generated for future use by the mobile device. Storing data in memory is a well-known conventional task and thus, a POSITA would have been successful storing the fake ID in memory. See claim 27 (§IX.F.1).

5. Claim 28

Claim 28	The system of claim 24, wherein the at least one access point includes a Wi-Fi access point, and wherein the at least one
----------	---

communication interface is configured for communication with a
Wi-Fi network.

655. In my opinion, *Vardi*, *IEEE802.11*, *Orava*, *Yun*, and *Kholaiif* render obvious claim 28. *See* claim 28 (§XI.A.19).

656. *Kholaiif* teaches “mobile station... comprises... a WLAN communication interface 30... WLAN communication interface 30 comprises a baseband processor 32 coupled to a radio 34, which in turn is coupled to an antenna 36.” *Id.*, ¶[242], Figure 27.

657. *Kholaiif*’s APs “jointly support a WLAN.” *Id.*, ¶[47].

658. A POSITA would have looked to and for components that support IEEE 802.11 standard communications when deploying mobile devices in a *IEEE802.11* WLAN and would have found success implementing them because that is one of the main purposes of a standard, ensuring compliance and compatibility. *See* Section IX.F.1.

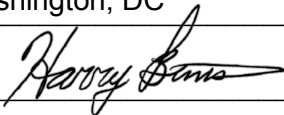
XIII. CONCLUSION

659. It is my opinion as an expert in telecommunications that the methods and systems recited in the claims 1-28 of the ’552 patent are unpatentable as obvious to a POSITA at the time of the claimed subject matter.

I, Harry V. Bims, do hereby declare and state, that all statements made herein of my knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, under Section 1001 of Title 18 of the United States Code and may jeopardize the validity of the application or any patent issuing thereon.

Executed on: September 3, 2024

Location: Washington, DC

By: 

Harry V. Bims, Ph.D.

Appendix A – Listing of the Claims

Element Designation	Claim Language
Claim 1	
[1pre]	1. A method performed by a server, the method comprising:
[1a]	transmitting, by the server to a device, an authenticated access point list that includes at least one of a media access control (MAC) address or a service set identifier (SSID) of each of one or more authenticated access points, wherein the one or more authenticated access points are controlled by the server; and
[1b]	transmitting, by the server to the device, a fake device identifier, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame in a search for at least one of the one or more authenticated access points around the device.
Claim 2	
[Claim 2]	The method of claim 1, wherein the one or more authenticated access points include a Wi-Fi access point.
Claim 3	
[Claim 3]	The method of claim 1, wherein the transmitting the fake device identifier includes transmitting a fake media access control (MAC) address.
Claim 4	
4[pre]	A method performed by an access point, the method comprising:

4[a]	receiving, by the access point from a device, a probe request frame that includes a fake device identifier for the device, wherein the fake device identifier is received at the device from a server, and wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;
4[b]	transmitting, by the access point to the device, a probe response frame that includes information regarding the access point;
4[c]	receiving, by the access point from the device in response to the transmitting the probe response frame, a connection request that includes an authentic device identifier for the device, wherein the receiving the connection request includes receiving the connection request in response to an authentication of the access point based on an authenticated point list received at the device from the server, and wherein the authenticated point list includes information that indicates that the access point is an authenticated access point; and
4[d]	transmitting, by the access point to the device in response to the receiving the connection request, an approval of the connection request, wherein the access point is controlled by the server.
Claim 5	
5[a]	The method of claim 4, further comprising: receiving, from the device, an association request;
5[b]	transmitting, to the device, an association response to the association request; and
5[c]	facilitating connection of the device to a communication network via the access point in accordance with the association response.
Claim 6	
[Claim 6]	The method of claim 5, wherein the access point includes a Wi-Fi access point, and wherein the communication network includes a Wi-Fi network.

Claim 7	
[Claim 7]	The method of claim 4, wherein the access point was previously communicatively coupled with the device.
Claim 8	
[Claim 8]	The method of claim 4, wherein the authentic device identifier includes a media access control (MAC) address of the device.
Claim 9	
[Claim 9]	The method of claim 4, wherein the information regarding the access point includes at least one of a media access control (MAC) address of the access point or a service set identifier (SSID) of the access point.
Independent Claim 10	
10[pre]	A method performed by a device, the method comprising:
[10a]	receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
[10b]	receiving, from the server, a fake device identifier for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame;
[10c]	transmitting, to at least one access point, the probe request frame that includes the received fake device identifier;
[10d]	receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;

[10e]	determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server; and
10[f]	transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.
Claim 11	
[Claim 11]	The method of claim 10, wherein the receiving the fake device identifier includes receiving a fake media access control (MAC) address.
Claim 12	
[Claim 12]	The method of claim 10, wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list comprises determining whether the at least one access point is under control of the server.
Claim 13	
[Claim 13]	The method of claim 10, further comprising: storing the authenticated access point list in a memory.
Claim 14	
14[pre]	The method of claim 10, further comprising:
14[a]	receiving, from the at least one access point, an approval of the connection request;

14[b]	transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;
14[c]	receiving, from the at least one access point, an association response to the association request; and
14[d]	connecting to a communication network via the at least one access point in accordance with the association response.
Independent Claim 15	
15[pre]	A method performed by a device, the method comprising:
15[a]	receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
15[b]	generating a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;
15[c]	transmitting, to at least one access point, a probe request frame that includes the fake device identifier;
15[d]	receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;
15[e]	determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list

	includes determining whether the at least one access point is under control of the server; and
15[f]	transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.
Claim 16	
[Claim 16]	The method of claim 15, wherein the generating the fake device identifier includes generating a fake media access control (MAC) address.
Claim 17	
[Claim 17]	The method of claim 15, wherein the information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access point or a service set identifier (SSID) of the at least one access point.
Claim 18	
[Claim 18]	The method of claim 15, wherein the determining whether the at least one access point is the authenticated access point further includes determining whether the at least one access point was previously connected with the device.
Claim 19	
[Claim 19]	The method of claim 15, further comprising: storing the authenticated access point list, received from the server, in a memory.
Claim 20	
20[pre]	The method of claim 15, further comprising:
[20a]	receiving, from the at least one access point, an approval of the connection request;

[20b]	transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;
[20c]	receiving, from the at least one access point, an association response to the association request; and
[20d]	connecting to a communication network via the at least one access point in accordance with the association response.
Independent Claim 21	
21[pre]	A method performed by a device, the method comprising:
21[a]	receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
21[b]	generating a collection that includes at least one of one or more random numbers or one or more random characters to provide a fake device identifier for the device to falsely identify the device in a probe request frame;
21[c]	transmitting, in a search for at least one available access point around the device, the probe request frame that includes the fake device identifier;
21[d]	receiving, from at least one access point around the device in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;

21[e]	determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of the server; and
21[f]	transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.
Claim 22	
22[pre]	The method of claim 21, wherein:
22[a]	the generating the collection that includes the at least one of one or more random numbers or one or more random characters comprises configuring the collection as a fake media access control (MAC) address, and
22[b]	the fake device identifier includes the fake media access control (MAC) address.
Claim 23	
[Claim 23]	The method of claim 21, further comprising: storing the fake device identifier in a memory.
Independent Claim 24	
24	A system, comprising:
24[a]	a processor;

24[b]	at least one communication interface;
24[c]	a transmitter to transmit, to at least one access point via the at least one communication interface, a probe request frame that includes a fake device identifier for a device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;
24[d]	a receiver to:
24[d][i]	receive, from the at least one access point via the at least one communication interface, a probe response frame that includes information regarding the at least one access point; and
24[d][ii]	receive, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
24[e]	a memory to store the information regarding the at least one access point, and the authenticated access point list; and
24[f]	a determination unit to determine, under control of the processor and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point and is under control of the server,
24[g]	wherein to determine whether the at least one access point is the authenticated access point and is under control of the server, the determination unit determines whether the information regarding the at least one access point is included in the authenticated access point list, and
24[h]	wherein the transmitter further transmits to the at least one access point, a connection request that includes an authentic device identifier for the device, in response to a determination by the determination unit that the at least one access point is the authenticated access point and is under control of the server.

Claim 25	
[Claim 25]	The system of claim 24, wherein the fake device identifier includes a fake media access control (MAC) address.
Claim 26	
[Claim 26]	The system of claim 24, further comprising: a fake device identifier generation unit to generate, under control of the processor, the fake device identifier.
Claim 27	
[Claim 27]	The system of claim 24, wherein the memory further stores the fake device identifier.
Claim 28	
[Claim 28]	The system of claim 24, wherein the at least one access point includes a Wi-Fi access point, and wherein the at least one communication interface is configured for communication with a Wi-Fi network

Appendix B – *Curriculum Vitae*

Dr. Harry V. Bims
Protocomm Systems, LLC
2665 Marine Parkway, Suite 1140
Mountain View, CA 94043
harrybims@me.com
650-283-4174

PROFESSIONAL SUMMARY

Harry Bims, PhD, EE, provides expert witness support services for telecommunications-related intellectual property litigation. These services include deposition and court testimony, expert reports, and infringement research, for patent, copyright, and trade secret litigation matters. He has 30+ years of telecommunications industry experience, and holds twenty-two US patents in network architecture and chip design for wireless communications.

EMPLOYMENT HISTORY

12/2001 - 05/2004 AirFlow Networks, Inc. LLC • Sunnyvale, California

Position: *CEO/CTO & Founder*

As the sole founder of the company, created the original business plan, raised venture capital, and hired the core engineering team. Grew the company to 32 people and shipped products for revenue in the US and overseas. Fifteen patents on the core technology have issued. These patents, which relate to wireless network infrastructure based on the 802.11 specification, have been sold to Broadcom.

03/2001 - 12/2001 Bay Partners LLC • Cupertino, California

Position: *Entrepreneur in Residence*

Reported to the partners of this VC firm as a technology expert on a range of wireless and networking subjects. Reviewed business plans and participated in due diligence activities related to several startups seeking funding. Developed a business plan for a startup that builds network infrastructure for 802.11 enterprise networks.

09/1999 - 03/2001 Symmetry Communications Systems LLC • San Jose, California

Position: *Director, Software Architecture*

Reporting to the CEO, responsible for the software architecture of their core SGSN and GGSN products for the GPRS market. Formulated a software technology roadmap, showing the evolution from 2.5G to 3G SGSN and GGSN products. Management responsibility for Firmware, Hardware, Performance, and Systems Engineering Groups. Provided management support of early field trials of the system on a global basis.

07/1999 - 09/1999 **T-SPAN Systems Corporation LLC • Palo Alto, California**

Position: *Member of Technical Staff*

Designed a wireless home LAN protocol for the company. Also designed and built a PC-based platform to demonstrate their technology. Company is now publicly traded as Atheros Communications.

07/1992 - 12/1998 **Glenayre Technologies-Wireless Access Group • San Jose, California**

Position: *Member of Technical Staff; Sr. Member of Technical Staff; Manager of NOC Systems*

Employee #6 at the company, which was acquired by Glenayre Technologies, Nov 1997. Designed and built a 4-channel ReFLEX50 pager demonstration in 1 week. Participated in early field trials and feasibility studies, culminating in a Pioneer's Preference license award from the FCC to SkyTel Corporation for Narrowband PCS development.

Invented, designed, and built from concept through full implementation, a patented two-way pager test system for the ReFLEX50 and ReFLEX25 protocols. This system was used throughout company operations for performance testing of the ReFLEX pager designs from Wireless Access, and Motorola. Over 16 systems were deployed around the country for manufacturing tests, engineering protocol tests, antenna tests, and pager repair tests.

The project required technical skills in PC hardware design, C++, object-oriented programming, signal processing techniques, NT device driver development, Win32 user interface development, real-time, multi-threaded control, and proficiency with wireless communications lab equipment. Three patents have been issued based on technical inventions in this capacity.

Co-developed a wireless application protocol for sending and receiving encrypted email messages over the paging channel. Led the project team that deployed a software encryption module based on this protocol for government agencies.

8/2018 – Present **CUPP Cybersecurity, LLC • Palo Alto, California**

Position: *CEO*

Developing a suite of network security products and technologies aimed at consumers to protect their online internet access.

10/2012 – Present **BoughtStuff, Inc • Palo Alto, California**

Position: *Founder*

The company has developed a mobile application for storage and delivery of product information to smartphones over wireless networks.

Bims Laboratories, Inc Work History

6/2009 – 7/2009 **Eastman Kodak Company • Rochester, NY**

Position: *Technology Consultant*

Providing technology assessment on certain wireless communication patents.

10/2009 – 1/2017 **IEEE 802.16 Working Group**

Position: *Task Group Secretary, Task Group Vice-Chair, Task Group Chair, Working Group Vice-Chair & Secretary, IEEE 802.16 Expert*

Served in several leadership capacities within this group that is working on improvements to the IEEE 802.16 standard, otherwise known as WiMAX. The 802.16 Working Group entered hibernation on March 2018. From that time until the present, I am on the roster of Experts designated by the Chair to answer questions and provide clarification about the 802.16 standards.

2/2014 – Present **Access Network Protocol Development**

Position: *Technical Lead Developer*

Developing a C++17-based DES of SDRs for wired and wireless network protocols, that includes IMT-2020 channel models. Implementations of the IEEE 802 and LTE protocol families, plus PTP, PPoE, IPv6, digital cable, Bluetooth, DSL, frame relay and many other managed node models for smart grid and vertical IoT applications. Used for technical analysis of emerging wireless standards amendments.

Protocomm Systems, LLC Consulting History

04/1999–07/1999 **Gigabit Wireless, Inc. • San Jose, California**

Position: *Technical Leader*

Technical leader for the Wireless MAC design group. Responsible for comparative analysis of competing wireless MAC protocol standards. Responsible for the creation of a proprietary MAC protocol specification document, simulation of the protocol, and implementation in a prototype. Participated in early 802.16 protocol standards. This company was acquired by Intel Corporation.

3/2007 – 10/2009 **Apple, Inc. • Cupertino, CA**

Position: *Technology Consultant*

Participating in IEEE 802.16 standards meetings as an affiliate of the client.

7/2003 – Present **Various expert witness engagements (see below)**

Position: *Technical Expert Witness*

Testified as a wireless technology expert in patent infringement cases. For a list of such cases, see below.

Technical Expert Witness Experience

03/2024 – Present **Client: Fish & Richardson, LLP (representing General Motors Company, and General Motors LLC (“GM”), Tesla Inc., and American Honda Motor Co., Inc., and Honda Development & Manufacturing of America, LLC (“Honda”))**

Client: DLA Piper LLP (representing Toyota Motor North America, Inc., Toyota Motor Sales, U.S.A., Inc., and Toyota Motor Engineering & Manufacturing North America, Inc., and Toyota Motor Credit Corporation (“Toyota”))

Client: Venable LLP (representing FCA US LLC)

Client: Brooks Kushman LLP (representing Ford Motor Co.)

Client: Jenner & Block LLP (representing Nissan North America Inc. and Nissan Motor Acceptance Corporation A/K/A Nissan Motor Acceptance Company LLC (“Nissan”))

Case: Neo Wireless, LLC v GM, Tesla, Honda, Toyota, FCA US LLC, Ford Motor Co., and Nissan, Civil Action No. 2:22-MD-03034-TGB (E.D. Mich)

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MICHIGAN SOUTHERN DIVISION

Testifying expert in this District Court matter involving 5G communications.

Expert Report:

March 28, 2024 Opening Expert Report on Invalidity

April 25, 2024 Rebuttal Expert Report on Non-Infringement

May 23, 2024 Expert Deposition

Attorneys: For Plaintiff:

For Defendant: Fish & Richardson, LLP, DLA Piper LLP, Venable LLP, Broosk Kushman LLP, Jenner & Block LLP

Status: Case ongoing

3/2024 – Present **Client: Finnegan, Henderson, Farabow, Garrett, & Dunner, LLP (representing Motorola Mobility LLC)**

Case: Lenovo (UNITED STATES) Inc. and Motorola Mobility LLC (Petitioners) v. Headwater Research LLC. (Patent Owner)

IPR Petition relating to Headwater Research LLC v Motorola Mobility LLC and Lenovo (United States) Inc. Case No. 4:23-cv-04496-JST (N.D. Cal.)

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARDa

Testifying expert in these matters involving application-level prioritization across networks.

April 17, 2024 Expert Declaration ISO IPR Petition regarding US Patent 9,198,076

July 17, 2024 Expert Declaration ISO IPR Petition regarding US Patent 10,749,700

July 15, 2024 Expert Declaration ISO IPR Petition regarding US Patent 9,198,076

August 8, 2024 Expert Declaration regarding US Patent 9,198,076

Attorneys: For Patent Owner:

For Petitioner: Finnegan

Status: Case ongoing

2/2024 – Present **Client: Bookoff McAndrews LLP (representing Motorola Mobility, LLC)**

Case: Patent Litigation between Ericsson and Motorola/Lenovo in Colombia

Location Testifying expert in these matters involving 5G networking technology.

Expert Declaration:

March 4, 2024 (COLOMBIA) Non-Essentiality and Non-Infringement
Technical Opinion regarding CO38083

March 20, 2024 (COLOMBIA) Invalidity Technical Opinion regarding
CO38001

March 27, 2024 (COLOMBIA) Non-Infringement Technical Opinion regarding
CO38001

March 27, 2024 (COLOMBIA) Non-Infringement Technical Opinion regarding
CO36031

March 27, 2024 (COLOMBIA) Non-Infringement Technical Opinion regarding
CO37362

April 16, 2024 (COLOMBIA) Non-Infringement and Non-Essentiality
Technical Opinion regarding CO37550

April 19, 2024 (COLOMBIA) Non-Essentiality Technical Opinion regarding
CO38002

July 19, 2024 (COLOMBIA) Invalidity Technical Opinion Regarding
CO38457

Attorneys: For Plaintiff:

For Defendant: Bookoff McAndrews, LLP

Status: Case ongoing

2/2024 – Present **Client: Fish & Richardson, LLP (representing Lenovo (United States))**

Case: Certain Cellular Base Station Communication Equipment, Components Thereof,
and Products Containing Same

U.S. Int'l Trade Commission Inv. No. 337-TA-1388

U.S. Int'l Trade Commission Inv. No. 337-TA-1397

Location: UNITED STATES INTERNATIONAL TRADE COMMISSION –

Administrative Law Judge Hon. MaryJoan McNamara
Testifying expert in this patent case involving 5G networking technology
August 7, 2024 Declaration Regarding Claim Construction

Attorneys: For Plaintiff:
For Defendant: Fish & Richardson
Status: ITC case ongoing

2/2024 – Present **Greenberg Traurig LLP (representing Samsung)**

Case: Samsung Electronics Co., Ltd., (Petitioner) v. Asus Technology Licensing Inc. (Patent Owner), IPR2024-00614
Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD
Testifying expert in this patent case involving LTE networking technology
March 8, 2024: PTAB Declaration ISO IPR petition
August 12, 2024: PTAB Declaration ISO IPR petition – US Patent 10,785,759
Attorneys: For Patent Owner:
For Petitioner: Greenberg Traurig LLP
Status: Case ongoing

7/2022 – Present **Client: Fish & Richardson LLP (representing LG Electronics, Inc.)**

Case: LG Electronics, Inc. v Invention Investment Fund I, L.P., Invention Investment Fund II, LLC, Intellectual Ventures I, LLC, and Intellectual Ventures II, LLC., Civil Action No. N22C-11-145-SKR-CCLD
Location: SUPERIOR COURT FOR THE STATE OF DELAWARE
Hon.
Testifying expert in these matters relating to a breach of a License Agreement
April 19, 2024: Opening Expert Report
Attorneys: For Plaintiff: Fish & Richardson LLP
For Defendant:
Status: Case ongoing

1/2024 – Present **Client: Kramer Levin Naftalis & Frankel, LLP (representing Acceleration Bay, LLC.)**

Case: Acceleration Bay, LLC v Amazon Web Services, Inc.

Civil Action No.: 22-904-RGA-SRF

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
– Hon. Richard G. Andrews

Testifying expert in this patent case involving internet data broadcasting.

Expert Declaration:

February 12, 2024: Expert Report Regarding Technology Tutorial of Asserted Patents

May 27, 2024 Live Deposition Testimony

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant: Fisch Sigler LLP

Status: Jury Award

12/2023 – Present **Kirkland & Ellis LLP (representing Motorola Mobility LLC & Lenovo)**

Case: Certain Mobile Phones, Components Thereof, and Products Containing the Same
U.S. Int'l Trade Commission Inv. No. 337-TA-1375

Certain Electronic Devices, including Mobile Phones, Tablets, Laptops,
Components Thereof, and Products Containing the Same
U.S. Int'l Trade Commission Inv. No. 337-TA-1376

Telefonaktiebolaget LM Ericsson v Lenovo (United States), Inc.
Civil Action No. 5:23-cv-569 (E.D.N.C.)

Lenovo (United States) v Telefonaktiebolaget LM Ericsson
Civil Action No. 5:23-cv-570 (E.D.N.C.)

IPR Petition Lenovo (United States) Inc. (Petitioner) v Telefonaktiebolaget LM
Ericsson (Patent Owner)

Location: UNITED STATES INTERNATIONAL TRADE COMMISSION
Administrative Law Judge Hon. MaryJoan McNamara

Testifying expert in this patent case involving 5G networking technology.

April 30, 2024 Expert Report on Invalidity

May 14, 2024 Rebuttal Expert Report Regarding Non-Infringement

May 31, 2024 Deposition Testimony

July 12-15, 2024 Live Testimony at Trial

Attorneys: For Plaintiff:

For Defendant: Kirkland & Ellis LLP

Status: Decision pending

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF
NORTH CAROLINA

Attorneys: For Plaintiff:

For Defendant: Kirkland & Ellis LLP

Status: Case ongoing

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF
NORTH CAROLINA

Testifying expert in this patent case involving establishing point-to-point
connections between mobile devices.

Attorneys: For Plaintiff: Kirkland & Ellis LLP

For Defendant:

Status: Case ongoing

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD
Case IPR2024-TBD

March 15, 2024: Declaration in support of Petition for IPR

Attorneys: For Petitioner: Kirkland & Ellis LLP

For Patent Owner:

Status: Case ongoing

12/2023 – Present **Fish & Richardson LLP (representing Reolink)**

Case: IPR Petition Shenzhen Reolink Technology Co., Ltd., Reolink Innovation Inc.,
Reolink Innovation Co., Ltd. (China) (Patent Owner) v Throughtek, Co., Ltd.
(Patent Owner), Attorney Docket No. 52472-0005IP1

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

January 29, 2024: PTAB Declaration ISO IPR petition

Attorneys: For Patent Owner:

For Petitioner: Kirkland & Ellis LLP

Status: Case ongoing

7/2023 – Present **Client: Finnegan, Henderson, Farabow, Garrett, & Dunner, LLP
(representing MediaTek)**

Case: U.S. Int'l Trade Commission Inv. No. 337-TA-1367

Certain Electronic Devices and Semiconductor Devices having Wireless
Communication Capabilities and Components Thereof

Location: UNITED STATES INTERNATIONAL TRADE COMMISSION –
Administrative Law Judge Hon. Bryan F. Moore

Testifying expert in this patent case involving IEEE 802.11 technology.

Expert Reports:

January 18, 2024 Rebuttal expert Report regarding Non-infringement

Videotaped Deposition:

February 15, 2024 Videotaped expert deposition

ITC Trial testimony:

March 24, 2024 Non-infringement witness statement

Attorneys: For Plaintiff:

For Defendant: Finnegan

Status: ITC case ongoing

8/2023 – Present **Kirkland & Ellis LLP (representing TP-Link Technologies Co Ltd.)**

Case: U.S. Int'l Trade Commission Inv. No. 337-TA-1361

In the Matter of Certain Wi-Fi Routers, Wi-Fi Devices, Mesh Wi-Fi Network
Devices, and Hardware and Software Components Thereof (ICC Case No.
27699/PDP)

Location: UNITED STATES INTERNATIONAL TRADE COMMISSION –
Administrative Law Judge Doris Johnson Hines

Testifying expert in these matters involving base station and wireless mesh
technology.

November 9, 2023: Expert report concerning Invalidity

November 30, 2023: Expert rebuttal report on Non-Infringement and Technical Domestic Industry

January 22, 2023: Live testimony at ITC trial

Attorneys: For Plaintiff: LLP

For Defendant: Kirkland & Ellis LLP

Status: Trial verdict pending

5/2023 – Present **Client: Fish & Richardson LLP (representing Samsung Electronics, Co. Ltd.)**

Case: In the Matter of an Arbitration Pursuant to the Rules of the International Court of Arbitration of the International Chamber of Commerce (ICC Case No. 27699/PDP)

Location: INTERNATIONAL CHAMBER OF COMMERCE

Testifying expert in these matters involving international patent arbitration between Interdigital and Samsung.

January 8, 2024 Rebuttal expert report

June 18, 2024 Second expert report

Attorneys: For Plaintiff: Alston & Bird LLP

For Defendant: Fish & Richardson LLP

Status: Case ongoing

10/2022 – 2/2023 **Client: Finnegan, Henderson, Farabow, Garrett & Dunner LLP (representing Samsung Electronics, Co. Ltd.)**

Case: IPR Petition relating to Apex Beam Technologies, LLC v. Samsung Electronics, Co. Ltd., Civil Action No. 2:22-cv-00188)

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in these matters involving smart antenna technology.

February 27, 2023: Expert Declaration ISO petition for Inter Partes review

February 28, 2023: “Xia” Expert Declaration ISO petition for Inter Partes review

February 28, 2023: “Liu” Expert Declaration ISO petition for Inter Partes review

Attorneys: For Patent Owner:
For Petitioner: Finnegan, Henderson, Farabow, Garrett & Dunner LLP
Status: Case settled

7/2022 – Present **Client: Russ, August & Kabat LLP (representing Vivato, Inc.)**

Case: XR Communications, LLC d/b/a Vivato Technologies v D-Link Systems, Inc.,
Civil Action No. 8:17-cv-00596-DOC(JDE)
Location: UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF
CALIFORNIA – Hon. David O. Carter
Testifying expert in these matters involving smart antenna technology.
Expert Declaration:
August 23, 2022: Rebuttal Expert Report on Validity
August 31, 2022: Deposition testimony
Attorneys: For Plaintiff: Russ, August & Kabat LLP
For Defendant:
Status: Case ongoing

6/2022 – 1/2024 **Client: Fish & Richardson LLP (representing Samsung Electronics, Co. Ltd.)**

Case: G+ Communications, LLC v Samsung Electronics Co. Ltd. et. al, Civil Action No.
2:22-cv-78
Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF
TEXAS – Hon. Rodney Gilstrap
Testifying expert in these matters involving smart antenna technology.
March 13, 2023: Expert Declaration ISO Samsung Defendants' Claim
Construction Proposals
June 28, 2023: Opening Expert Report on Invalidity
December 18, 2023: PTAB Declaration ISO IPR Petition
Attorneys: For Plaintiff: Russ, August & Kabat LLP
For Defendant: Fish & Richardson
Status: Jury trial verdict

5/2022 – 6/2023 **Client: Kilpatrick Townsend LLP (representing Apple, Inc.)**

Case: IPR Petition relating to Apple, Inc. v. Mullen Industries LLC, Civil Action No. 6:22-cv-00145

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in these matters involving remote notification devices.

August 8, 2022: Expert Declaration

May 23, 2023: Expert Deposition

Attorneys: For Patent Owner: Mintz, Levin, Cohn, Ferris, Glovsky, and Popeo, P.C.

For Petitioner: Kilpatrick Townsend LLP

Status: Case settled

3/2022 – 9/2023 **Client: Kirkland & Ellis LLP (representing Samsung Electronics Co. Ltd.)**

Case: California Institute of Technology v Samsung Electronics Co. Ltd., Civil Action No. 2:21-cv-00446

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS – Hon. Rodney Gilstrap

Testifying expert in these matters involving LDPC codes.

November 22, 2022: Declaration regarding claim construction

December 20, 2022: Rebuttal Declaration regarding claim construction

May 22, 2023: Rebuttal expert report on non-infringement

May 31, 2023: Deposition testimony

Attorneys: For Petitioner: Kirkland & Ellis LLP

For Plaintiff: Mintz, Levin, Cohn, Ferris, Glovsky, and Popeo, P.C.

Status: Case settled

2/2022 – 12/2022 **Client: Fish & Richardson LLP (representing Apple, Inc.)**

Case: Litigation between Ericsson and Apple in Belgium, Brazil, Germany, Netherlands, and Colombia, and US matters:

Ericsson Inc. et. al. v. Apple Inc., Civil Action No. 6:22-cv-00061-ADA

Ericsson Inc., et. al, v. Apple Inc., Civil Action No. 2:21-cv-00376

Apple Inc. v. Telefonaktiebolaget LM Ericsson, et. al., Civil Action No. 2:21-cv-00460

In the Matter of Certain Mobile Phones Tablet Computers, Smart Watches, Smart Speakers, and Digital Media Players, and Products Containing Same.

U.S. Int’l Trade Commission Inv. No. 337-TA-3596

Location: UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TEXAS WACO DIVISION – Hon. Alan D. Albright

UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS

UNITED STATES INTERNATIONAL TRADE COMMISSION

Testifying expert in these matters involving 5G networking technology.

Expert Declaration:

May 18, 2022 COLOMBIA: Invalidity and Non-Infringement Technical Opinion regarding certain Colombia patents

April 27, 2022 COLOMBIA: Invalidity and Non-Infringement Technical Opinion regarding certain Colombia patents #1

April 27, 2022 COLOMBIA: Invalidity and Non-Infringement Technical Opinion regarding certain Colombia patents #2

March 28, 2022 COLOMBIA: Invalidity and Non-Infringement Technical Opinion regarding certain Colombia patents

March 9, 2022 BRAZIL: Invalidity Technical Opinion regarding Brazil patents

May 26, 2022 BRAZIL: Response to Ericsson Statement regarding Brazil patents

August 25, 2022 BRAZIL: Live testimony before the Brazil Patent and Trademark Office regarding invalidity

November 15, 2022 (COLOMBIA) Invalidity and Non-Infringement Technical Opinion regarding CO37550

Attorneys: For Plaintiff:

For Defendant: Fish & Richardson, LLP

Status: Case settled

1/2022 – 3/2023 **Client: Finnegan LLP (representing Toyota Motor Corp., et. al.)**

Case: Intellectual Ventures I LLC, et. al. v. Toyota Motor Corp., et. al., Civil Action No. 2:21-cv-389

Toyota Motor Corp. (Petitioner) v. Intellectual Ventures II, LLC (Patent Owner)
Case No. IPR2022-01355

Location: UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TEXAS MARSHALL DIVISION –

UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in this District Court and PTAB matter involving IEEE 802.11 wireless networking.

Expert Declaration:

January 13, 2023: Marshall Division Declaration on Invalidity

August 25, 2022: PTAB Declaration ISO Petition for IPR

April 8, 2024: PTAB Declaration ISO Petition for IPR2022-00973

Attorneys: For Plaintiff:

For Defendant/Petitioner: Finnegan, LLP

Status: Case settled

9/2021 – Present **Client: Schulte, Roth & Zabel LLP (representing TrackThings LLC)**

Case: TrackThings LLC v. NETGEAR, Inc. Civil Action No. 22-981-RGA-JLH

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE –

Testifying expert in this District Court matter involving wireless network reconfiguration.

January 25, 2024: Expert report regarding infringement

July 9, 2024 Expert Rebuttal report regarding Validity of US Patent Nos. 9,642,017, 9,332,442, and 10,107,893

August 15, 2024 headReply Expert Report regarding infringement

Attorneys: For Plaintiff: Schulte, Roth, and Zabel

For Defendant: Quinn Emanuel

Status: Case ongoing

9/2021 – Present **Client: Stroock LLP/Schulte, Roth & Zabel (representing TrackThings LLC)**

Case: TrackThings LLC v. Amazon.com, Inc. and Amazon.com Services LLC, and eero LLC., Civil Action No. 6:21-cv-00720; Civil Action No. 6:23-cv-00133-ADA

Location: UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TEXAS WACO DIVISION – Hon. Alan D. Albright

Testifying expert in this District Court matter involving wireless network reconfiguration.

March 10, 2022: Expert declaration ISO claim construction responses

January 20, 2023 Expert report on Infringement

February 24, 2023 Rebuttal Expert report regarding Validity

February 9, 2024 Expert report regarding Infringement

March 8, 2024 Rebuttal Expert report regarding Validity

March 29, 2024 Live deposition testimony

Attorneys: For Plaintiff: Schulte, Roth, and Zabel

For Defendant: Quinn Emanuel

Status: Case ongoing

12/2020 – Present **Client: BlankRome (representing Samsung Electronics Co., Ltd)**

Case: TOT Power Control, S.L. v. Samsung Elecs. Co., Ltd and Samsung Elecs. Am. Inc., Civil Action No. 1:21-cv-01305-MN

IPR Petition relating to TOT Power Control, S.L. v. Samsung Elecs. Co., Ltd and Samsung Elecs. Am. Inc., Civil Action No. 1:21-cv-01305-MN

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
– Hon. Maryellen Noreika

UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this district court and IPR proceeding involving power control methods in wireless systems.

September 12, 2022: 865 Expert Declaration

Attorneys: For Plaintiff: DLA Piper
For Defendants: Blank Rome

For Patent Owner: Hausfeld, LLP
For Petitioner: Blank Rome

Status: Case ongoing

10/2021 – 5/2022 **Client: Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
(representing MediaTek Inc.)**

Case: NXP USA, Inc. v. MediaTek Inc., et. al., Civil Action No. 2:21-cv-000318-JRG –
Hon. Rodney Gilstrap

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF
TEXAS MARSHALL DIVISION

Testifying expert in this District Court matter involving 802.11n, 802.11ac, and
802.11ax chipsets.

Expert Report:

February 3, 2022 Declaration ISO Defendant's Claim Construction Brief

Attorneys: For Plaintiff: Duane Morris, LLP
For Defendant: Finnegan, LLP

Status: Case settled

09/2021 – Present **Client: Fish & Richardson, LLP (representing Samsung Electronics Co.,
Ltd., et. al.)**

Case: Smart Mobile Technologies, LLC v. Samsung Electronics Co., Ltd., et. al., Civil
Action No. 6:21-cv-00701-ADA. Hon. Alan D. Albright

Location: UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF
TEXAS WACO DIVISION

Testifying expert in this District Court matter involving wireless voice and data
transfer.

Expert Report:

June 8, 2022 Declaration ISO Defendant's Claim Construction Brief

Attorneys: For Plaintiff: Hagens Berman Sobol Shapiro, LLP
For Defendant: Fish & Richardson, LLP

Status: Case ongoing

05/2021 – 6/2021 **Client: Sidley Austin (representing HP Inc. and Microsoft Corporation)**

Case: SynKloud Technologies, LLC v. HP Inc., Civil Action No. 1:19-cv-01360-RGA
and Microsoft Corporation v. SynKloud Technologies, LLC, Civil Action No.
1:20-cv-00007-RGA

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE

Testifying expert in this District Court matter involving wireless cloud storage.

Expert Report:

June 25, 2021 Declaration ISO Microsoft and HP's Claim Construction Brief

Attorneys: For Plaintiff:

For Defendant: Sidley Austin

Status: Case settled

05/2021 – 5/2022 **Client: DLA Piper (representing Motorola Mobility LLC)**

Case: U.S. Int'l Trade Commission Inv. No. 337-TA-1253
Certain LTE-Compliant Cellular Communication Devices
Motorola v. Evolved Wireless LLC.

Location: UNITED STATES INTERNATIONAL TRADE COMMISSION –
Administrative Law Judge Cameron R. Elliot

Testifying expert in this ITC matter involving LTE cellular device handover.

Expert Report:

November 16, 2021 Expert Report on NonInfringement and Lack of Technical
Domestic Industry

Expert Testimony:

December 15, 2021 Deposition testimony

Attorneys: For Plaintiff: Nelson Bumgardner Albritton P.C.; Adduci, Mastriani & Schaumberg, LLP

For Defendant: DLA Piper

Status: Case settled

04/2021 – 6/2022 **Client: Desmarais LLP (representing Google LLC and FitBit Inc.)**

Case: Cellspin Soft, Inc. v. Fitbit, Inc., No. 4-17-cv-05928-YGR

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA

Hon. Yvonne Gonzalez Rogers

Testifying expert in this patent case involving the distribution of real-time health data.

Expert Testimony:

October 29, 2021 Expert Report on NonInfringement

Attorneys: For Plaintiff: Garteiser Honea PLLC and Corcoran IP Law PLLC

For Defendant: Desmarais LLP

Status: Case settled. Summary Judgment for Non-Infringement.

3/2021 – 9/2021 **Client: Fish & Richardson (representing Samsung)**

Case: U.S. Int'l Trade Commission Inv. No. 337-TA-1248

Certain Cellular Communications Infrastructure Systems, Components Thereof, and Products Containing Same

U.S. Int'l Trade Commission Inv. No. 337-TA-DN-3525

Certain Cellular Communications Infrastructure Systems, Components Thereof, and Products Containing Same

Location: UNITED STATES INTERNATIONAL TRADE COMMISSION

Testifying expert in this ITC matter regarding 3GPP technology.

Attorneys: For Plaintiff: Winston & Strawn, LLP

For Defendant: Fish & Richardson, LLP

Status: Case terminated in its entirety based on an Initial Determination.

2/2021 – 11/2021 **Client: Fish & Richardson (representing Quectel)**
Client: Axinn, Veltrop & Harkrider LLP (representing Thales DIS AIS USA, LLC)
Client: Pearl Cohen LLP (representing Telit)
Case: U.S. Int’l Trade Commission Inv. No. 337-TA-1240
Certain UMTS and LTE Cellular Communication Modules and Products
Containing the Same
Koninklijke Philips N.V. v Quectel Wireless Solutions Co. Ltd., Thales DIS AIS
Deutschland GmbH, Thales S.A., Telit Wireless Solutions, Inc., Telit
Communications PLC, CalAmp Corp, Xirgo Technologies, LLC, Laird
Connectivity, Inc., Thales DIS AIS USA LLC
Case No. 1:20-cv-1713 (D. Del)
Location: UNITED STATES INTERNATIONAL TRADE COMMISSION –
Administrative Law Judge Hon. David P. Shaw
Testifying expert on 3GPP mobile device operation.
Expert Testimony:
July 21, 2021 Expert Report on Invalidity
August 6, 2021 Deposition Testimony
October 12, 2021 Live Testimony before ALJ David P. Shaw
Attorneys: For Plaintiff: Mayer Brown LLP
For Defendants: Fish & Richardson; Axinn, Veltrop & Harkrider LLP
Status: Case closed

11/2020– Present **Client: Orrick, Herrington & Sutcliffe LLP (representing PayPal Holdings, Inc.)**
Case: IOENGINE LLC v PayPal Holdings, Inc.
Civil Action No. 1:18-cv-00452-WCB
Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
Hon. William C. Bryson
Testifying expert in this patent case involving peripheral device communication
to remote servers.
Expert Testimony:
November 19, 2021 Expert Report on Invalidity

January 7, 2022 Expert Report on Non-Infringement
January 20-21, 2022 Deposition Testimony on Invalidity and Non-Infringement
Status: Case ongoing

11/2020 – Present **Client: DLA Piper (representing Apple, Inc.)**

Case: Maxell v. Apple Inc. In the Matter of Certain Mobile Electronic Devices and Laptop Computers

U.S. Int'l Trade Commission Inv. No. 337-TA-1215

Location: UNITED STATES INTERNATIONAL TRADE COMMISSION –
Administrative Law Judge Hon. Dee Lord

Testifying expert on 3GPP mobile device operation.

Expert Testimony:

February 25, 2021: Opening Expert Report Regarding Invalidity

March 11, 2021: Rebuttal Expert Report regarding NonInfringement and Lack of Technical Domestic Industry

March 24, 2021: Videotaped deposition

Attorneys: For Plaintiff: Mayer Brown LLP

For Defendant: DLA Piper LLP

Status: Case settled

11/2020– 11/2020 **Client: Folio Law Group PLLC (representing Dali Wireless)**

Case: Dali Wireless, Inc. v. John Mezzalingua Associates, LLC d/b/a JMA Wireless and Teko Telecom SRL (an Italian Corporation)

Civil Action No. 19-2367-RGA

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE

Testifying expert in this patent case involving distributed antenna system networks.

Expert Testimony:

November 6, 2020: Declaration Regarding Interpretation of Asserted Claims

Status: Case closed

8/2020– 8/2022 **Client: Folio Law Group PLLC (representing Dali Wireless)**

Case: Dali Wireless, Inc. v. Corning Optical Communications, LLC,
Civil Action No. 3:20-cv-06469-EMC

Location: UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF
TEXAS – Hon. Edward M. Chen

Testifying expert in this patent case involving distributed antenna system
networks.

Expert Testimony:

February 12, 2021: Declaration Regarding Interpretation of Asserted Claims

June 29, 2022: Expert Report on Infringement

August 22, 2022: Deposition Testimony

October 11, 2022: Supplemental Expert Report on Infringement

Status: Case closed

3/2020– 8/2021 **Client: Folio Law Group PLLC (representing Dali Wireless)**

Case: Dali Wireless, Inc. v. CommScope Technologies, LLC and CommScope Holding
Company, Inc..

Civil Action No. 1:19-cv-00952-MN

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
– Hon. Maryellen Noreika

Testifying expert in this patent case involving distributed antenna system
networks.

Expert Testimony:

June 23, 2021: Expert report on infringement.

August 17, 2021: CORRECTED Reply Expert report on infringement of '338
Patent

Status: Case closed

03/2020 – 8/2022 **Client: Sidley Austin LLP (representing Lenovo and Motorola)**

Case: InterDigital Technology Corporation, IPR Licensing, Inc., InterDigital
Communications, Inc., InterDigital Holdings, Inc., and InterDigital, Inc. v.
Lenovo Holding Company, Inc., Lenovo (United States) Inc., and Motorola
Mobility LLC

Civil Action No. 19-1590-LPS

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
Hon. Leonard P. Stark

Testifying expert in this patent case involving 3G and 4G cellular standards.

Expert Testimony:

April 16, 2022 Expert report on Invalidity of '665 and '954 patents

June 16, 2022 Expert Report on Invalidity of 8,675,612 and 9,456,449 patents

June 16, 2022 Rebuttal Expert Report on Invalidity of 8,085,665 and
8,427,954 patents

July 17, 2022 Rebuttal expert report regarding non-infringement of '612
and '449 patents

July 18, 2022 Rebuttal expert report on non-infringement of '665 and '954
patents

August 8, 2022 Rebuttal Expert Report on Invalidity of '612 and '449 patents

August 31, 2022 Videotaped expert Deposition

Status: Case closed

3/2020– 5/2022 **Client: Finnegan, Henderson, Farabow, Garrett & Dunner LLC
(representing Google)**

Case: IPR Petition Google LLC, v. Sonos, Inc., Case No. IPR2021-01563

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving wireless home speaker
systems.

Expert Testimony:

September 27, 2021: Declaration ISO petition for Inter Partes Review

May 10, 2022: Supplemental declaration ISO petition for Inter Partes Review

June 29, 2022: Videotaped deposition testimony

Status: Case closed

08/2019 – 6/2021 **Client: Fish & Richardson (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Cisco, Inc.

Civil Action No. 5:17-cv-00072-BLF-SVK

Location: UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF CALIFORNIA SAN DIEGO DIVISION – Hon. Susan Van Keulen

As a testifying expert, provided a technology tutorial in this patent case involving internet security technology.

Expert Testimony:

August 14, 2019 Tutorial expert report on network security technology.

September 4, 2019 Deposition Testimony

Attorneys: For Plaintiff: Fish & Richardson

For Defendant:

Status: Case settled

8/2019 – 5/2020 **Client: Fish & Richardson (representing LG Electronics, Inc.)**

Case: Bell Northern Research, LLC v. LG Electronics, Inc., et. al.

USDC-SDCA Civil Action No. 18-cv-2864-CAB-BLM

Location: UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF CALIFORNIA – Hon. Cathy Ann Bencivengo, Magistrate Judge: Hon. Barbara L. Major

Testifying expert on wired/wireless communication in gaming systems.

Expert Testimony:

November 20, 2019 Declaration ISO motion for summary judgment

Attorneys: For Plaintiff: Skiermont Derby LLP

For Defendant: Fish & Richardson

Status: Case closed

7/2019 – 05/2021 **Client: O'Melveny & Myers LLP (representing Apple Inc.)**

Case: Maxell, Ltd. v. Apple Inc.,

Case No. 5:19-cv-00036-RWS.

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS TEXARKANA DIVISION – Hon. Robert W. Schroeder III

Testifying expert on 3G cellular telephone technology.

Expert Testimony:

May 7, 2020: Opening Expert Report Regarding Invalidity
June 4, 2020: Rebuttal Expert Report on Non-Infringement
Deposition Testimony: June 24, 2020
Attorneys: For Plaintiff: Mayer Brown LLP
For Defendant: O'Melveny & Myers LLP
Status: Case settled.

4/2019 – Present **Client: Perkins Coie (representing Nintendo of America, Inc.)**

Case: Genuine Enabling Technology LLC v. Nintendo Company Ltd., and Nintendo of America, Inc., W.D. Wash.,

Civil Action No. 2:19-cv-00351-RSM

Location: UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON – Hon. Ricardo S. Martinez

Testifying expert on wired/wireless communication in gaming systems.

Expert Declarations:

October 23, 2019 Declaration ISO claim constructions

November 26, 2019 Sur-reply declaration ISO claim constructions

January 23, 2020 Declaration ISO motion for summary judgment

April 20, 2020 Opening Expert Report Regarding Invalidity

Expert Depositions:

December 19, 2019

Claim Construction Hearing Testimony:

February 24, 2020 Tutorial testimony on the technology of the Asserted Patents

Attorneys: For Plaintiff: Bayard, P.A.

For Defendant: Perkins Coie

Status: Case ongoing

12/2019 – 12/2019 **Client: Erise IP (representing Apple Inc.), Haynes and Boone, LLP (representing Ericsson Inc)**

Case: Ericsson Inc. (Petitioner) v. Uniloc 2017, LLC (Patent Owner)

Apple Inc. (Petitioner) v. Uniloc 2017, LLC (Patent Owner) Case No. IPR2020-

00224

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving ARQ data exchange on LTE
networks.

Expert Declarations:

December 16, 2019 Declaration ISO Petition for Inter Partes Review of U. S.
Patent No. 7,075,917

Attorneys: For Petitioner: Erise IP; Haynes and Boone, LLP

For Patent Owner:

Status: Case closed

6/2019 – 7/2020 **Client: Fish & Richardson (representing Microsoft Corporation)**

Case: Microsoft Corp. (Petitioner) v. Uniloc 2017, LLC (Patent Owner)

Uniloc 2017, LLC v. Microsoft Corp.

USDC Central District of California, Case Nos. 8:18-cv-2053, 8:18-cv-2054,
8:18-cv-2224; 8:19-cv-0428, 8:19-cv-0477, 8:19-cv-0196

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving 3GPP transport formats and
channels.

Expert Declarations:

August 6, 2019 Declaration in support of claim construction

Attorneys: For Plaintiff: Feinberg Day LLP

For Defendant: Fish & Richardson

Status: Case settled

2/2019 – 5/2020 **Client: Klarquist Sparkman, LLP (representing Microsoft Corporation)**

Case: Uniloc 2017, LLC v. Microsoft Corp.

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving ARQ data exchange on LTE
networks.

Expert Declarations:

April 14, 2019 Declaration ISO Petition for Inter Partes Review of U. S.
Patent No. 7,075,917

Attorneys: For Plaintiff:

For Defendant: Klarquist LLP

Status: Case settled

10/2018 – 6/2021 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Eset, Inc.

Civil Action No. 3:17-cv-00183-CAB-BGS

Location: UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF
CALIFORNIA SAN DIEGO DIVISION – Hon. Cathy Ann Bencivengo

As a testifying expert, provided a technology tutorial in this patent case involving
internet security technology.

Expert Declaration:

October 5, 2018 Tutorial expert report on network security technology.

March 11, 2020 Jury trial testimony.

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant:

Status: Jury Trial Mistrial due to COVID-19.

Case closed.

9/2018 – 6/2021 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Juniper, Inc.

Civil Action No. 15-cv-03295-BLF-SVK

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF
CALIFORNIA SAN JOSE DIVISION – Hon. Beth L. Freeman

As a testifying expert, provided a technology tutorial in this patent case involving
internet security technology.

Expert Declaration:

September, 11, 2018 Tutorial expert report on network security technology.

Videotaped Deposition:

November 7, 2018

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant:

Status: Case closed

9/2017 – 9/2018 **Client: (Covington & Burling representing Huawei Device USA, Inc.)**

Case: Optis Wireless Technology, LLC, et. al. v. Huawei Technologies Co. Ltd, et. al.

Civil Action No. 2:17-cv-123-JRG-RSP

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS MARSHALL DIVISION – Hon. Roy S. Payne

Testifying expert regarding 3G and LTE technology.

Expert Declarations and Reports:

November 3, 2017: Declaration regarding Claim Construction.

March 26, 2018: Initial Expert Report Regarding Invalidity

April 23, 2018: Rebuttal Expert Report on Non-Infringement

April 27, 2018: Rebuttal Expert Report on Secondary Considerations

Videotaped Deposition: May 10, 2018

May 14, 2018: Declaration in support of Motion for Partial Summary Judgment

Jury Trial Testimony: August 22, 2018 and August 23, 2018

Attorneys: For Plaintiff: McKool Smith

For Defendant: Covington & Burling

Status: Jury award

6/2017 – 4/2018 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Symantec, Inc.

Civil Action No. 4:14-cv-02998-HSG

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA OAKLAND DIVISION

As a testifying expert, provided a technology tutorial in this patent case involving

internet security technology.

Expert Declaration:

July 27, 2017 Tutorial expert report on security technology.

Videotaped Deposition:

August 29, 2017

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant: Quinn Emmanuel

Status: Case settled

5/2017 – 3/2018 **Client: Barnes & Thornburg, LLP (representing Ooma, Inc.)**

Case: Ooma, Inc. (Petitioner) v. Deep Green Wireless, LLC (Patent Owner)

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

As a testifying expert, provided a technology tutorial in this patent case involving
voice and data communications over wireless networks.

Expert Declaration:

June 8, 2017 Expert report on prior art wireless network technology.

Videotaped Deposition:

February 15, 2018

Attorneys: For Petitioner: Barnes & Thornburg LLP

For Defendant: Mischcon De Reya New York, LLP

Status: Case closed

3/2017 – 6/2019 **Client: Fish & Richardson (representing Apple, Inc.) / Gibson, Dunn &
Crutcher LLP (representing Compal Electronics, et. al.)**

Case: Apple Inc. v. Qualcomm Inc.

Qualcomm Inc. v. Compal Electronics, Inc., et. al.

Civil Action No. 3:17-cv-00108 / Civil Action No. 3:17-cv-01010

Location: UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF
CALIFORNIA – Hon. Gonzalo P. Curiel, Magistrate Judge: Hon. Mitchell D.
Dembin

Testifying expert regarding LTE technology.

Expert Declaration:

December 11, 2017: Declaration regarding Claim Construction.

Expert Report:

June 29, 2018: Opening Expert Report regarding invalidity

August 3, 2018: Expert Report on infringement

October 2, 2018: Rebuttal Expert Report on Invalidity

Videotaped Deposition:

October 25, 2018

None

Attorneys: For Apple: Fish & Richardson

For Qualcomm: Quinn Emanuel Urquhart & Sullivan LLP / Cravath, Swaine & Moore LLP

For Compal Electronics, Inc., et. al: Gibson, Dunn & Crutcher LLP

Status: Case settled.

3/2017 – 1/2018 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Blue Coat Systems, LLC

Civil Action No. 15-cv-03295-BLF-SVK

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA SAN JOSE DIVISION – Hon. Beth L. Freeman

As a testifying expert, provided an opening technology tutorial at trial in this patent case involving internet security technology.

Expert Declaration:

March 29, 2017 Tutorial expert report on security technology.

Videotaped Deposition:

May 2, 2017

October 31 – November 2, 2017: Jury Trial Testimony

January 8-10, 2018: Jury Trial Testimony (retrial after mistrial):

Live Testimony on Network Security Technology Tutorial

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant: Morrison & Forrester & Quinn Emmanuel

Status: Jury award

1/2017 – 7/2017 **Client: Foster Pepper LLP (representing Dali Wireless)**

Case: Dali Wireless, Inc. (Petitioner) v. CommScope Technologies, LLC (Patent Owner)

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in this patent case involving RF transport networks.

Expert Reports:

4-26-17 Declaration ISO petition for IPR

6-30-17 Declaration ISO Opening claim construction brief

Videotaped Deposition:

July 24, 2017

Status: Case closed

1/2017 – 6/2019 **Client: Dorsey & Whitney LLP (representing Dali Wireless)**

Case: CommScope Technologies, LLC (Plaintiff/Counterclaim Defendant) v. Dali Wireless, Inc. (Defendant/Counterclaim Plaintiff)

Civil Action No.: 3:16-cv-477

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF TEXAS DALLAS DIVISION

– Hon. Barbara M. G. Lynn

Testifying expert in this patent case involving RF transport networks.

Expert Reports:

8-24-18 Expert Report regarding Invalidity of CommScope patents

8-24-18 Expert Report regarding Infringement of Dali Wireless patents

11-5-18 Expert Report regarding Validity of Dali Wireless patents

11-5-18 Expert Report regarding Non-Infringement of CommScope patents

1-9-19 Declaration ISO opposition to MSJ

1-18-19 Declaration ISO partial MSJ on Non-infringement and Invalidity

5-2-19 Declaration ISO Motion for Sanctions

Videotaped Deposition:

November 20, 2018

Live Testimony at Jury Trial:

June 10-13, 2019

Attorneys: For Plaintiff: Dorsey & Whitney, LLC

For Defendant: Carlson Caspers, P.A.

Status: Jury award.

11/2016 – 4/2019 **Client: Boies, Schiller & Flexner LLP (representing Apple Inc.)**

Case: Evolved Wireless, LLC v. Apple, Inc.

Civil Action No.: 1:15-cv-00542-SLR

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
– Hon. Sue L. Robinson

Testifying expert in this patent case involving LTE wireless networks.

Expert Reports:

11-06-17 Declaration ISO Summary Judgment of Validity

10-05-17 Declaration ISO Summary Judgment of Non-Infringement

10-03-17 Supplemental Expert Report on Non-Infringement

07-24-17 Supplemental Expert Report on Secondary Considerations of Non-Obviousness

6-26-17 Expert Report on Non-Infringement

5-22-17 Expert Report on Invalidity

Videotaped Deposition:

August 11, 2017

Live Testimony at Jury Trial:

March 29 - April 1, 2019

Attorneys: For Plaintiff: Boies, Schiller & Flexner LLP

For Defendant: Robins Kaplan LLP

Status: Jury verdict of non-infringement.

7/2016 – 4/2018 **Client: Jackson Walker LLP (representing D&M Holdings, Inc., et. al.)**

Case: Sonos, Inc., v. D&M Holdings, d/b/a The D+M Group, D&M Holdings U.S. Inc.,

and Denon Electronics (USA), LLC

Civil Action No.: 16-0141-RGA

D&M Holdings Inc., d/b/a The D+M Group, D&M Holdings U.S. Inc. v. Sonos, Inc.

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
– Hon. Richard G. Andrews

Testifying expert in this patent case involving wireless speaker networks.

Expert Testimony:

9-11-17 Expert Report on Infringement

6-29-22 Remote Videotaped Deposition

Attorneys: For Plaintiff: Jackson Walker LLP

For Defendant: Potter Anderson & Corroon LLP

Status: Case settled

7/2016 – 1/2018 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Palo Alto Networks, Inc. (Petitioner) v. Finjan, Inc. (Patent Owner)

Case IPR2015-02001, Case IPR2016-00157. US Patent No. 8,225,408 B2

Case IPR2015-01974

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this patent case involving wireless speaker networks.

Expert Declaration:

8-9-16 Expert Declaration, Patent 7,647,633

8-9-16 Expert Declaration, Patent 8,225,408

8-30-16 Supplemental Expert Declaration, 7,647,633

Status: Case settled

5/2016 – 7/2018 **Client: (Winston & Strawn LLP representing Atlantic Broadband Group, LLC, et. al.)**

Case: ChanBond LLC v. Atlantic Broadband Group, LLC, et. al.

Civil Action No: 15-842-RGA, 15-843-RGA, 15-844-RGA, , 15-845-RGA, , 15-846-RGA, , 15-847-RGA, , 15-848-RGA, , 15-849-RGA, , 15-850-RGA, , 15-851-RGA, , 15-852-RGA, , 15-853-RGA, , 15-854-RGA

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
– Hon. Richard G. Andrews

Testifying expert regarding digital cable technology.

Expert Report:

10-24-17 Expert Report on Invalidity

Videotaped Deposition:

None

Attorneys: For Plaintiff: Bayard, P.A.

For Defendant: Winston & Strawn LLP

Status: Case settled

5/2016 – 11/2019 **Client: (Torys LLP representing Telus, Bell, and Rogers)**

Case: Wi-LAN Inc. v Telus Communications Company, Rogers Communications
Canada Inc., and Bell Mobility Inc.

Court File No. T-301-16; Court File No. T-303-16; Court File No. T-304-16

Location: CANADIAN FEDERAL COURT – Hon. Mandy Ayles

Testifying expert regarding LTE technology.

Expert Report:

June 14, 2019 Expert Report regarding invalidity

Videotaped Deposition:

None

Attorneys: For Plaintiff: Torys LLP

For Defendant:

Status: Case settled

12/2015 – 4/2016 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Acceleration
Bay, LLC.)**

Case: Activision Blizzard, Inc., Electronic Arts Inc., Take-Two Interactive Software,
Inc., 2K Sports, Inc., Rockstar Games, Inc., and Bungie, Inc., Petitioner v.
Acceleration Bay, LLC, Patent Owner.

Case IPR2015-01951, Case IPR2015-01953, Case IPR2015-01964, Case
IPR2015-01970, Case IPR2015-01996, Case IPR2016-00724, Case IPR2016-
00747

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR patent case involving internet data broadcasting.

Expert Declaration:

January 4, 2017 Supplemental Declaration ISO Patent Owner's Response -- Case
IPR2016-00724

January 4, 2017 Supplemental Declaration ISO Patent Owner's Response -- Case
IPR2016-00747

December 7, 2016 Declaration ISO Patent Owner's Response – Case IPR2016-
00724; Secondary Considerations of Non-Obviousness

December 7, 2016 Declaration ISO Patent Owner's Response – Case IPR2016-
00747; Secondary Considerations of Non-Obviousness

July 17, 2016 Declaration ISO Patent Owner's Response – Patent 6,714,966;
Secondary Considerations of Non-Obviousness

July 17, 2016 Declaration ISO Patent Owner's Response – Patent 6,829,634;
Secondary Considerations of Non-Obviousness

July 17, 2016 Declaration ISO Patent Owner's Response – Patent 6,701,344;
Secondary Considerations of Non-Obviousness

Videotaped Deposition:

February 7, 2017 and February 8, 2017

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant: Winston & Strawn

Status: Cased closed

4/2016 – Present **Client: Kramer Levin Naftalis & Frankel, LLP (representing Acceleration
Bay, LLC.)**

Case: Acceleration Bay, LLC v Activision Blizzard, Inc., Electronic Arts Inc., Take-
Two Interactive Software, Inc.

Civil Action No.: 14-453 (RGA), 16-454 (RGA), 16-455 (RGA)

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
– Hon. Richard G. Andrews

Testifying expert in this patent case involving internet data broadcasting.

Expert Declaration:

September 24, 2017: Expert Report Regarding Technology Benefits of the Asserted Patents

Videotaped Deposition: January 4, 2018

July 17, 2018: Reply Report Regarding Technology Benefits of the Asserted Patents

April 29 – May 3, 2024 Live Tutorial Testimony at Trial about benefits of Asserted Patents

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant: DLA Piper

Status: Jury Award

12/2015 – 9/2016 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Sophos, Inc.

Civil Action No. 3:14-cv-01197-WHO

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA SAN FRANCISCO DIVISION – Hon. William H. Orrick

As a testifying expert, provided a technology tutorial in this patent case involving internet security technology.

Expert Declaration:

December 21, 2015 Tutorial expert report on network security technology.

Videotaped Deposition:

February 22, 2016

September 5 – 9, 2016 Jury Trial:

Live Testimony at Jury Trial regarding tutorial on network security

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant: DLA Piper

Status: Jury Trial

9/2015 – 2/2016 **Client: Brinks Gilson & Lione (representing LifeWatch Services, Inc., and Card Guard Scientific Survival, Ltd.)**

Case: Card Guard Scientific Survival Ltd.

Reexam Control No. 12/706,541

Location: UNITED STATES PATENT AND TRADEMARK OFFICE
Provided testimony in this Patent Office re-examination appeal.

Expert Declaration:

November 13, 2015 Declaration under 37 C.F.R §1.132.

February 13, 2016 Declaration ISO petition for IPR.

Attorneys: For Plaintiff: Brinks Gilson & Lione

Status: Re-examination appeal decision invalidated the patent.

9/2015 – 1/2017 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Proofpoint, Inc. and Armorize Technologies, Inc.

Civil Action No. 13:cv-03999-BLF

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA SAN JOSE DIVISION – Hon. Howard R. Lloyd, Hon. Haywood S. Gilliam, Jr.

As a testifying expert, provided an opening technology tutorial report in this patent case involving internet security technology.

Expert Declaration:

October 7, 2015 Tutorial expert report on network security technology.

Videotaped Deposition:

November 6, 2015

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant: Quinn Emanuel

Status: Case settled

8/2015 – 12/2015 **Client: Brinks Gilson LLP (representing ZTE Corporation and ZTE (USA), Inc.)**

Case: Inter-System Handover of a Mobile Terminal Operable with a First and a Second Radio Access Network

ZTE v. Vringo Infrastructure, Inc.

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving 3GPP cellular technology.

Expert Declarations:

08-28-15 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 7,126,940

09-04-15 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 7,242,943

09-04-15 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 7,558,283

09-04-15 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 8,812,000

09-04-15 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 7,724,720

10-12-15 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 7,242,933

Videotaped Deposition:

None

Attorneys: For Plaintiff:

For Defendant: Brinks Gilson, LLP

Status: Case settled.

11/2014 – Present **Client: Fish & Richardson (representing Regents of the University of Minnesota)**

Case: Regents of the University of Minnesota v. AT&T Mobility, LLC, Sprint Solutions, Inc., T-Mobile USA, Inc., Cellco Partnership d/b/a Verizon Wireless
Civil Action No. 14-cv-4666

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MINNESOTA
– Hon. Tony N. Leung

Testifying expert on 3GPP error correction coding, precoding, and modulation.

May 12, 2023: Expert Deposition

April 14, 2023: Rebuttal Expert Report regarding Validity

Attorneys: For Plaintiff: Fish & Richardson

For Defendant:

Status: Case ongoing

10/2014 – 2/2015 **Client: Alston & Bird (representing Microsoft Corporation)**

Case: Microsoft Corporation. v. IPR Licensing, Inc.

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving cellular technology.

Expert Declarations:

10-16-14 Supplemental Declaration ISO Petition for Inter Partes Review of U.
S. Patent No. 8,380,244

Attorneys: For Plaintiff: Alston & Bird LLP

For Defendant:

Status: Case settled

9/2014 – 4/2015 **Client: Reed & Scardino, LLP (representing Mobile Telecommunications Technologies, LLC)**

Case: Mobile Telecommunications Technologies LLC v. Amazon.com, Inc.

Civil Action No. 2:13-CV-883-JRG-RSP

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF
TEXAS MARSHALL DIVISION – Hon. Roy S. Payne

Testifying expert in this patent case involving package delivery notification
systems and reliable delivery of wireless messages.

Expert Reports:

4-06-15 Second Supplemental Expert Report on Infringement

2-10-15 Expert Report on Infringement

2-24-15 Supplemental Expert Report on Infringement

Videotaped Deposition:

2-25-15

Declaration:

3-20-15 Declaration ISO Response to Opposition Motion

Attorneys: For Plaintiff: Reed & Scardino LLP
For Defendant: Greenberg Traurig LLP
Status: Case settled

5/2014 – 7/2015 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Blue Coat Systems, Inc.
Civil Action No. 3:13-cv-03999-BLF

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA SAN JOSE DIVISION – Hon. Beth L. Freeman

As a testifying expert, provided an opening technology tutorial at trial in this patent case involving internet security technology.

Expert Declaration:

January 12, 2015 Tutorial expert report on security technology.

Videotaped Deposition:

March 18, 2015

Live Jury Trial Testimony: July 20, 2015.

Live Bench Trial on Laches Testimony: September 8, 2015

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP
For Defendant: Wilson Sonsini

Status: Jury award.

4/2014 – 12/2014 **Client: Reed & Scardino, LLP (representing Mobile Telecommunications Technologies, LLC)**

Case: Mobile Telecommunications Technologies LLC v. United Parcel Service, Inc.
Civil Action No. 1:12-cv-03222-AT

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION – Hon. Amy Totenberg

Testifying expert in this patent case involving package delivery notification systems.

Expert Reports:

7-3-14 Opening Expert Report regarding Infringement

8-11-14 Rebuttal Expert Report regarding Infringement

Videotaped Depositions:

10-7-14

Declaration:

11-24-14 Declaration ISO Response to MSJ

Attorneys: For Plaintiff: Reed & Scardino LLP

For Defendant: Alston & Bird LLP

Status: Case settled.

12/2013 – 9/2015 **Client: Brinks Gilson & Lione LLP (representing ZTE Corp, and ZTE (USA), Inc.)**

Case: ZTE Corporation and ZTE (USA) Inc. v. InterDigital Technology Corporation

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving cellular technology.

Expert Declarations:

3-21-14 Declaration in support of the Petition for Inter Partes Review of U. S.
Patent No. 8,380,244

Attorneys: For Plaintiff: Brinks Gilson & Lione

For Defendant: Latham & Watkins, LLP

Status: IPR Hearing before PTAB: All disputed claims are unpatentable.

12/2013 – 4/2014 **Client: Kramer Levin Naftalis & Frankel LLP (representing Sirius XM Radio Inc.)**

Case: Catch a Wave Technologies, Inc. v. Sirius XM Radio Inc.

Case No. 3:12-cv-05791-WHA

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF
CALIFORNIA SAN FRANCISCO DIVISION – Hon. William Alsup

Testifying expert in this patent case involving satellite radio systems.

Expert Reports:

2-14-2014 Expert Report regarding non-infringement

Attorneys: For Plaintiff: Freitas Tseng & Kaufman LLP
For Defendant: Kramer Levin LLP
Status: Case settled

2/2013 – 7/2016 **Client: Reed & Scardino, LLP (representing Mobile Telecommunications Technologies, LLC)**

Case: Mobile Telecommunications Technologies LLC v. BlackBerry Corporation.
Civil Action No. 3:12-cv-1652-M

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF TEXAS DALLAS DIVISION – Hon. Barbara M. G. Lynn

Testifying expert in this patent case involving package delivery notification systems.

Expert Reports:

9-3-15 Expert Report on Infringement

Videotaped Depositions:

November 18, 2015

Live Testimony at Jury Trial: July 13, 2016.

Attorneys: For Plaintiff: Baker Botts, LLP
For Defendant: Reed & Scardino LLP
Status: Jury verdict of non-infringement.

9/2013 – 1/2014 **Client: Reed & Scardino, LLP (representing Mobile Telecommunications Technologies, LLC)**

Case: Mobile Telecommunications Technologies, LLC v Clearwire Corporation
Civil Action No. 2:12-CV-308

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS MARSHALL DIVISION – Hon. Roy S. Payne

Testifying expert in this patent case involving wireless networking signals.

Expert Reports:

11-11-13 Rebuttal report regarding validity

Videotaped Depositions:

12-5-13

Declarations:

1-23-14 Declaration before the Patent Trial and Appeal Board in Case IPR2013-00306

Attorneys: For Plaintiff: Reed & Scardino LLP
For Defendant: Shook, Hardy & Bacon, LLP

Status: Case settled

10/2013 – 5/2015 **Client: Foley & Lardner, LLP (representing Motorola Mobility, LLC)**

Case: University of Florida Research Foundation Inc., and Rapid Mobile Technologies, Inc. v Motorola Mobility, LLC.

Case No. 13-cv-61120-KMM-EGT

Location: UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF FLORIDA FORT LAUDERDALE DIVISION – Hon. K. Michael Moore,
Magistrate Judge: Hon. Edwin G. Torres

Testifying expert in this patent case involving mobile device testing systems.

Expert Reports:

None.

Declarations:

11-21-13 Declaration ISO Motorola's Responsive Claim Construction Brief

Attorneys: For Plaintiff: Meltzer & Meksraitis
For Defendant: Foley & Lardner LLP

Status: Case settled

7/2013 – 6/2015 **Client: WilmerHale (representing Broadcom)**

Case: Inter Partes Review of US Patent 6,424,625; 6,772,215; and 6,466,568 owned by Ericsson

Docket No. 0111168-0240

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in this Inter Partes Review regarding ARQ mechanisms.

Expert Declarations:

9-19-13 Declaration regarding US Patent 6,772,215

9-19-13 Declaration regarding US Patent 6,466,568

9-29-13 Declaration regarding US Patent 6,424,625

Videotaped Deposition:

5-29-14, and 5-30-14

Attorneys: For Plaintiff: Meltzer & Mathis

For Defendant: Wilmer Cutler Pickering Hale and Dorr LLP

Status: IPR Petition granted. All claims invalidated

4/2013 – 4/2015 **Client: Kilpatrick Townsend & Stockton LLP (representing Google Inc. and Motorola Mobility LLC)**

Case: Fujifilm Corporation v. Motorola Mobility LLC

Case No. 3:12-cv-03587 WHO

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA SAN FRANCISCO DIVISION – Hon. Richard Seeborg

Testifying expert in this patent case involving smartphone technology and video codecs.

Expert Declarations:

4-23-14 Declaration ISO Motion for Protective Order

12-9-14 Declaration ISO MSJ

Expert Reports:

10-3-14 Opening Expert Report Regarding Invalidity

10-31-14 Rebuttal Expert Report on non-infringement

10-31-14 Appendix A to Rebuttal Report of Dr. Alan Bovik

Videotaped Deposition:

11-19-14, and 11-20-14

Trial Testimony:

April 28, 2015 Non-infringement and invalidity of '970 Patent

Attorneys: For Plaintiff: Morgan, Lewis & Bockius LLP

For Defendant: Kilpatrick Townsend & Stockton LLP

Status: Jury verdict: '970 Patent claims not infringed and invalid.

2/2013 – 10/2013 **Client: Seyfarth Shaw LLP (representing Motorola Mobility LLC)**

Case: University of Florida Research Foundation, Inc. and Rapid Mobile Technologies, Inc. v. Motorola Mobility LLC

Civil Action No. 13-cv-61120-KMM-EGT

Location: UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF FLORIDA – Hon. K. Michael Moore, Magistrate Judge: Hon. Edwin G. Torres

Testifying expert in this employment law case involving mobile device testing systems.

Expert Reports:

3-1-13 Expert Report regarding Non-Infringement

4-1-13 Declaration in Opposition to Plaintiff's MSJ

Attorneys: For Plaintiff: Meltzer & Mathis

For Defendant: Seyfarth Shaw LLP

Status: Case settled

5/2012 – 4/2013 **Client: Paul Hastings LLP (representing Apple, Inc.)**

Case: SmartPhone Technologies, LLC v Research in Motion Corporation, et. al.

Case No. 6:10-cv-00074

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS TYLER DIVISION – Hon. John D. Love

Testifying expert in this patent case involving 3GPP technology.

Expert Reports:

12-31-12 Appendix A to Rebuttal Expert Report of Dr. David Wilson

3-13-13 Appendix A to Supplemental Expert Report of Dr. David Wilson

Attorneys: For Plaintiff: Mintz Levin Cohn Ferris Glovsky and Popeo PC

For Defendant: Paul Hastings LLP

Status: Case settled

8/2012 – 9/2013 **Client: Reed & Scardino, LLP (representing EON Corp. IP Holdings, LLC)**

Case: EON Corp. IP Holdings, LLC v. SKYGUARD, LLC et. al.

Case No. 6:11-cv-00015-LED

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS TYLER DIVISION – Hon. John D. Love

Testifying expert in this patent case involving RF technology for WiFi networking.

Expert Reports:

2-15-13 Expert Report regarding Infringement

Videotaped Deposition:

4-09-13

Attorneys: For Plaintiff: Reed & Scardino, LLP

For Defendant: K&L GATES LLP

Status: Case settled

5/2012 – 6/2014 **Client: Reed & Scardino LLP (representing Eon Corp. IP Holdings)**

Case: Eon Corp. IP Holdings, LLC v. Landis+Gyr, Inc., et. al.

Case No. 6:09-cv-00317-LED-JDL

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS TYLER DIVISION – Hon. John D. Love

Testifying expert in this patent case involving two-way wireless networks, before Judge Love.

Expert Report:

7-8-13 Expert Report regarding Infringement by Silver Spring Networks, Inc.

7-8-13 Expert Report regarding Infringement by Itron, Inc.

Videotaped Deposition: September 12, 2013

Live Testimony at Jury Trial: June 2, 2014 – June 6-2014

Attorneys: For Plaintiff: Reed & Scardino LLP

For Defendant: Dentons, LLP

Status: Jury award. All patents found valid and infringed.

3/2012 – 3/2014 **Client: Perkins Coie (representing Intel Corporation)**

Case: Stragent LLC, et. al. v. Intel Corp.,

Case No. 6:11-cv-421-LED (E.D. Tex.)

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS TYLER DIVISION – Hon. Timothy Dyk, Hon. John D. Love

Testifying expert in this patent case involving the use of error detection technology in computer networking, before Judge Dyk.

Expert Reports:

08-23-13 Expert Report regarding Invalidity

09-23-13 Expert Report regarding Non-Infringement

Videotaped Deposition:

10-08-13, and 10-09-13

Jury trial testimony:

3-13-2014 Live trial testimony on non-infringement and invalidity before Judge Timothy Dyk

Attorneys: For Plaintiff: Nelson, Bumgardner & Casto

For Defendant: Perkins Coie

Status: Jury verdict for non-infringement and invalidity

2/2012 – 09/2015 **Client: Dewey & LeBoeuf LLP (representing Harris Corporation)**

Case: Harris Corporation v. Ruckus Wireless, Inc.

Case No. 6:11-cv-00618-CEM-CRS

Location: UNITED STATES DISTRICT COURT FOR THE MIDDLE DISTRICT OF FLORIDA ORLANDO DIVISION – Hon. Charlene Edwards Honeywell

Testifying expert in this patent case involving RF technology for WiFi networking.

Expert Reports:

3-5-12 Expert Report regarding Infringement

3-6-12 Supplemental Expert Report regarding Infringement

4-6-12 Expert Report regarding Validity

Declarations:

5-30-12 Declaration ISO Claim Construction

6-18-12 Declaration ISO Markman Motion

1-23-15 Declaration ISO Responsive Markman Brief

3-6-15 Supplemental Expert Report regarding Infringement

4-3-15 Rebuttal Expert Report regarding Validity

Videotaped Deposition:

4-30-12

Attorneys: For Plaintiff: Dewey & LeBeouf LLP

For Defendant: Lewis and Roca LLP

Status: Case settled

2/2012 – 2/2013 **Client: Common-Interest-Group (representing Nokia, Huawei, ZTE)**

Case: InterDigital Communications LLC, et. al. v. Huawei Tech Co., LTD., et. al.

Certain Wireless Devices With 3G Capabilities and Components Thereof

U.S. Int'l Trade Commission Inv. No. 337-TA-800

Location: UNITED STATES INTERNATIONAL TRADE COMMISSION –
Administrative Law Judge Hon. David P. Shaw and Administrative Law Judge
Hon. Theodore R. Essex

Testifying expert in this patent case involving 3G wireless, WiFi, and WCDMA
technology.

Expert Reports:

11-30-12 Expert Report regarding Non-infringement

7-31-12 Expert Report regarding Invalidity

11-19-10 Rebuttal Expert Report regarding Validity

12-6-10 Supplemental Expert Report regarding Infringement

Videotaped Deposition:

12-14-12, 12-15-12

ITC Trial testimony:

2-6 through 2-15/13 Non-infringement and Invalidity witness statements, live
testimony

Attorneys: For Plaintiff: Latham & Watkins, LLP

For Defendant: Alston & Bird, Covington & Burling, Brinks Hofer

Status: ITC hearing verdict: All patents not infringed and invalid

9/2010 – 4/2011 **Client: Reed & Scardino LLP (representing Eon Corp. IP Holdings)**

Case: Eon Corp. IP Holdings, LLC v. Sensus USA, Inc., et. al.
Case No. 6:09-cv-00116-LED-JDL
Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS
TYLER DIVISION – Hon. John D. Love
Testifying expert in this patent case involving two-way wireless networks
Expert Report:
10-22-10 Expert Report regarding Infringement (Sensus USA, Inc)
11-7-10 Expert Report regarding Infringement (Bell Industries)
11-19-10 Rebuttal Expert Report regarding Validity
12-6-10 Supplemental Expert Report regarding Infringement
Declaration:
12-28-10, 1-18-11
Videotaped Deposition:
12-8-10, 2-3-11
Attorneys: For Plaintiff: Reed & Scardino LLP
For Defendant: Jones Day
Status: Case settled

10/2009 – 2/2010 **Client: White & Case LLP (representing Marvell)**

Case: Marvell Semiconductor, Inc., et. al. v. Commonwealth Scientific Industrial
Research Organisation
Case No. 6:07-CV-204 (LED)
Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS
TYLER DIVISION – Hon. Leonard Davis
Testifying expert in this patent case involving wireless LAN protocols.
Expert Report:
11-24-09 Rebuttal Expert Report
Videotaped Deposition:
01-07-10
Attorneys: For Plaintiff: White & Case LLP
For Defendant: Townsend and Townsend and Crew LLP
Status: Case settled

9/2009 – 2/2010 **Client: Perkins Coie Brown & Bain PA (representing Intel)**

Case: Saxon Innovations, LLC v. Apple, Inc., et. al.

Case No. 6:08-cv-00265-LED

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS TYLER DIVISION – Hon. John D. Love

Testifying expert in this patent case involving wireless technology.

Declarations:

12-04-09 Declaration Regarding Claim Construction

Videotaped Deposition:

01-19-10

Attorneys: For Plaintiff: Susman Godfrey LLP

For Defendant: Perkins Coie Brown & Bain LLP

Status: Case settled

8/2008 – 10/2009 **Client: Reed & Scardino LLP (representing Eon Corp. IP Holdings)**

Case: Eon Corp. IP Holdings, LLC v. Verizon Clinton Center Drive Corp., et. al.

Case No. 6:08-cv-00385

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS TYLER DIVISION – Hon. John D. Love

Testifying expert in this patent case involving two-way wireless networks

Expert Report:

06-22-10 Expert Report

08-16-10 Supplemental Expert Report

Videotaped Depositions:

08-18-10, 08-26-10

Attorneys: For Plaintiff: Reed & Scardino LLP

For Defendant: Simpson Thacher & Bartlett LLP

Status: Case settled

4/2008 – 3/2009 **Client: McDermott, Will & Emery LLP (representing GE Licensing)**

Case: CIF Licensing, LLC d/b/a GE Licensing v. Agere Systems, Inc.

Case No. 07-170 (JJF)

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE

– Hon. Joseph. J. Farnan, Jr.

Testifying expert in this patent case involving modem technology.

Expert Report:

09-05-08 Rebuttal Expert Report

Non-videotaped Depositions:

9-24-08, 9-26-08

Jury trial testimony:

2-04-09

Attorneys: For Plaintiff: McDermott, Will & Emery LLP

For Defendant: Townsend and Townsend and Crew LLP

Status: Jury award. 2 patents infringed and valid, remaining 2 patents non-infringed

2/2008 – 5/2010, **Client: Simpson Thacher & Bartlett LLP (representing Cisco Systems, Inc.)**
2/2011 – 4/2011

Case: Commil USA, LLC v. Cisco Systems, Inc., et. al.

Case No. 2:07-CV-341-DF-CE

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS

MARSHALL DIVISION – Hon. Charles Everingham IV

Testifying expert on invalidity regarding short range communication protocols.

Opening Expert Report

12-23-09

Videotaped Depositions:

02-09-10

Attorneys: For Plaintiff: Sayles Werbner

For Defendant: Simpson Thacher & Bartlett LLP

Status: Jury award for original trial and retrial: patents found valid and infringed.

6/2007 – 4/2009 **Client: Common Interest Group of Co-Defendants**

11/2010 – 4/2012 **Client: Common Interest Group of Co-Defendants**

Case: Commonwealth Scientific and Industrial Research Organisation v. Toshiba America Information Systems, Inc., et. al.

Case No. 6:06-cv-00550-LED

Case No. 6:09-CV-0399 (LED)

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS
TYLER DIVISION – Hon. Leonard Davis

Testifying expert in this patent case involving wireless LAN technology.

Declarations:

06-05-08 Regarding claim construction

12-17-08 Supporting opposition to summary judgment

04-05-09 Supporting motion for reconsideration

02-24-12 Supporting opposition to summary judgment

Expert Reports:

10-08-08 Rebuttal Expert Reports- Re: TI Chips, Re: Marvell Chips, Re: Airgo Chips, Re: Broadcom Chips, Re: Conexant Chips, Re: Ralink Chips, Re: Atheros Chips

01-27-12 Rebuttal Expert Reports- Re: TI Chips, Re: Broadcom Chips, Re: Ralink Chips, Re: Atheros Chips

Videotaped Depositions:

11-1-08, 11-2-08, 02-14-12

Attorneys: For Plaintiff: Townsend & Townsend LLP

For Defendant: Keker & Van Nest, LLP

Status: Jury trial: patents found valid and infringed.

10/2006 – 8/2009 **Client: Keker & Van Nest (representing Comcast Corporation)**

Case: Rembrandt Technologies, Inc. v. Comcast Corporation

Case No. 2-05-CV-000443 (TJW)

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION – Hon. T. John Ward

Testifying expert in this patent case involving physical layer and data link layer communication protocols for cable networks.

Declaration:

01-10-07 Support of Claim Construction Brief

Videotaped Deposition:

12-22-06 Regarding claim construction opinions

Attorneys: For Plaintiff: McKool Smith

For Defendant: Keker & Van Nest

Status: Case settled

3/2007 – 5/2007 **Client: Niro, Scavone, Haller and Niro (representing MLR, LLC)**

Case: MLR, LLC v. Kyocera Wireless Corporation and Novatel Wireless, Inc.

Case No. 05-CV-0935 B (AJB)

Location: UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF CALIFORNIA

Testifying expert in this patent case involving cellular phone technology.

Expert Report:

04-20-07 Expert Report regarding infringement

Attorneys: For Plaintiff: Niro, Scavone, Haller, and Niro

For Defendant: Hogan & Hartson, LLP

Status: Case settled

6/2006 – 10/2006 **Client: Thompson & Knight (representing Ericsson, Inc.)**

Case: Fenner Investments, Ltd., v. Juniper Networks, Inc. et. al.

Case No. 2:05–CV–05 JDL

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS MARSHALL DIVISION

Testifying expert in this patent case involving wireless communications services.

Expert report regarding infringement and invalidity

5-23-06 Rebuttal expert report regarding infringement and invalidity

Attorneys: For Plaintiff: Fulbright & Jaworski

For Defendant Ericsson: Thompson & Knight

Status: Case settled

12/2003 – 5/2006 **Client: Howrey LLP/ Winston & Strawn LLP (representing McKesson Information Solutions, Inc.)**

Case: McKesson Information Solutions, Inc. vs. Bridge Medical, Inc.
Case No. CIV S-02-2669 FCD KJM

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF CALIFORNIA – Hon. Peter A. Nowinski

Testifying expert in this patent case involving a patient on a patient identification and verification system that incorporates wireless technology.

Inequitable Conduct Trial live testimony:
5-04-06

Markman Hearing live testimony:
6-29/30-05

Videotaped Depositions:
2-14-04, 6-3-05

Declarations:
12-1-03 Dec. in support of MISI's Opening/Opposition re Claim Construction
12-24-04 Dec. in support of MISI's Motion for Preliminary Injunction
3-1-04 Dec. in support of Claim Construction
6-29-04 Dec. re meaning of "Communication"
7/15/05 Dec. in support of MISI's Opposition to Bridge's Motion for Summary Judgment

Attorneys: For Defendant: Morrison & Foerster

For Plaintiff: Howrey Simon, Winston & Strawn, Morgan Lewis

Status: Bench trial on inequitable conduct: Verdict found inequitable conduct.

07/2003–02/2006 **Client: Heller Ehrman LLP (representing Texas Instruments, Inc.)**

Case: Texas Instruments, Inc. and Stanford University vs. GlobespanVirata, Inc.

Provided discovery of evidence used at trial, concerning the structure and operation of Globespan's ADSL products, and supported litigators in depositions of Globespan engineers.

Attorneys: For Plaintiff: Heller Ehrman

For Defendant: Covington & Burling, LLP

Status: Jury award.

Patents

<u>Patent Number</u>	<u>Date Issued</u>	<u>Title</u>
11,748,764	September 5, 2023	Light-based Data Entry for Personal Inventory and Product Support System
10,332,121	June 25, 2019	Light-based Data Entry for Personal Inventory and Product Support System
9,978,037	May 22, 2018	Personal inventory and product support system
8,995,996	March 31, 2015	Methods and apparatus for performance optimization of heterogeneous wireless system communities
8,935,580	January 13, 2015	Multimedia-aware quality-of-service and error correction provisioning
8,468,426	June 18, 2013	Multimedia-aware quality-of-service and error correction provisioning
8,189,538	May 29, 2012	Reconfiguration of a communication system
8,144,640	March 27, 2012	Location tracking in a wireless communication system using power levels of packets received by repeaters
8,064,380	November 22, 2011	Reconfiguration of a communication system
8,027,637	September 27, 2011	Single frequency wireless communication system
7,957,741	June 7, 2011	Token-based receiver diversity
7,876,704	January 25, 2011	Tunneling protocols for wireless communications
7,689,210	March 30, 2010	Plug-n-playable wireless communication system
7,672,274	March 2, 2010	Mobility support via routing
7,668,542	February 23, 2010	Token-based receiver diversity
7,515,557	Apr 7, 2009	Reconfiguration of a communication system
7,236,470	Jun 26, 2007	Tracking multiple interface connections by mobile stations
7,149,196	Dec 12, 2006	Location tracking in a wireless communication system using power levels of packets received by repeater
6,965,769	Nov 15, 2005	Testing Center
6,862,448	Mar 1, 2005	Token-based receiver diversity
6,788,658	Sep 7, 2004	Wireless communication system architecture having split MAC layer

6,760,318	Jul 6, 2004	Receiver diversity in a communication system
6,557,134	Apr 29, 2003	ARQ method for wireless communication
6,259,911	Jul 10, 2001	Network operations center hardware and software design

Education

<u>Year</u>	<u>College/University</u>	<u>Degree</u>
1993	Stanford University	PhD, Electrical Engineering Thesis: "Trellis Coding for Multi-Level, Partial-Response Continuous Phase Modulation with Precoding"
1988	Stanford University	MS, Electrical Engineering
1985	Rensselaer Polytechnic Institute	BS, Computer and Systems Engineering

Publications

Goldhamer, M., Grandblaise, D., Bims, H., Feng, S., Piggin, P., Sydor, J., and Wu, X. "Coexistence between 802.16 Systems Operating in Shared Bands", *Radio Resource Management in WiMAX*, John Wiley & Sons, 2009.

Bims, Harry. "Surveying the Wireless LANDscape. Or Why Large Wi-Fi Networks Require Good Planning." *Xchange*. [Online] Available <http://www.xchangemag.com/articles/391supsys1.html>, September 1, 2003.

Bims, Harry. "Building Voice-Ready Wireless LANs" *Wireless Week*. [Online] Available <http://www.wirelessweek.com/article/CA319429.html?spacedesc=Departments>, September 1, 2003.

Bims, Harry. "Enabling Voice over WLANs". White Paper. [Online] Available. http://airflownetworks.com/solutions/pdf/vowlan_wp.pdf. September 2003.

Bims, Harry. "Securing Enterprise WLANs". White Paper. [Online] Available. http://web.archive.org/web/20040303212529/airflownetworks.com/solutions/pdf/securing_wlans_wp.pdf. August 2003.

Bims, H. and Cioffi. J. "Trellis Coding for Full-Response CPM", *Third Generation Wireless Information Networks*, Kluwer Academic Publishers, 1992.

Bims, H. and Cioffi. J. "Trellis Coding for Full-Response CPM", *WINLAB WORKSHOP*, East Brunswick, NJ. October 18-19, 1990.

Bims, H. and Cioffi, J. “Trellis Coding for Partial-Response CPM”, *1991 International Symposium on Information Theory*, Budapest, Hungary. June 24-28, 1991.

Bims, H. and Cioffi, J. “Trellis Coding with M-ary MSK Constraints”, *GLOBECOM '89*, Dallas TX. Nov. 1989.

Professional Associations and Achievements

- Jan 2009 – Present Vice-Chair and Board of Directors, Menlo Park Chamber of Commerce
- Nov 2007 – Sep 2010 Vice-Chair and Secretary, IEEE 802.16h License Exempt Group
- Feb 2002 – Jan 2011 Member, City of Menlo Park Planning Commission
(2006 Chairperson, 2005 Vice-Chairperson)
- Feb 2012 – Present Senior Member, IEEE
- Jan 2000 – Dec 2000 Chair, IEEE Engineering Management Society – Silicon Valley Chapter
- Jun 1985 - Jun 1991 AT&T Bell Laboratories Cooperative Research Fellow